9

Systems and Equipment

The only thing constant in life is change.

François de la Rochefoucauld, author

Innovation is moving at an incredible rate and our industry is right in there reaping the benefits and pondering the questions plaguing so many industry managers. It seems as though as soon as you get the money to install a new gadget or system, it is redesigned the next year. We cannot always keep up fiscally and it may not be necessary. Some systems are absolute requirements while others are just more convenient. Be careful not to get so far behind the technology curve that you are not providing adequate security. The many systems used in the hospitality industry are not necessarily electronic in nature, but I have tried to spend some time and space here with at least a general overview so you will know what to look for in your systems.

FIRE ALARMS

Fire alarms are generally designed, installed, and maintained by an outside vendor or possibly another department, such as Facilities or Engineering. Some properties prefer to have the Security Director (Safety) responsible for the operation of this important system. No matter what your involvement in the fire system is, your department will definitely be involved when it activates, so some knowledge of how it works is required.

The basic fire system has two main objectives: notification and suppression. In other words, it should alert occupants and the fire department and put out the fire. The notification part of the system consists of automatic detectors, manual switches, the control panel, communications interface, and alert devices. The suppression system consists of detectors, water pumps, standpipes, chemical supplies, and sprinklers or chemical emitters. Remember, this is a general overview and your system may contain many more-complicated devices.

Automatic Detectors

The most common visual detector is the smoke or ion detector. This device is often mounted on the ceiling and looks and acts like the smoke detector in your home. It detects smoke with a photoelectric beam just like the one used in a store to alert the clerk of an entering customer. When smoke crosses the beam, a switch is activated. These are commonly tampered with by hotel guests who smoke in their rooms and can be activated in rare cases by an extremely steamy shower.

The ion detector is a bit more complicated to explain, but is also much cheaper and therefore more common. An ion detector uses an extremely small amount of radioactive material to ionize particles that enter a chamber. Smoke particles have a different value than regular oxygen particles do, so they are detected and the switch is activated. Ion detectors are considered better detectors because a fire with high flame has less smoke and sometimes it is not as quickly detected by photoelectric detectors.

Where steam or smoke may be normal, such as bathrooms and kitchens, heat sensors may be used. These simply activate the switch when the temperature in a room reaches a preset threshold.

Carbon monoxide detectors are less common in business applications, but may be used to detect the dangerous invisible gas emitted by gas engines and fires.

Suppression sprinklers, which are addressed later, also act as detectors and do not need any electricity to operate. A fire sprinkler is a valve attached to a water pipe in the ceiling. The valve is held closed by a mechanical detector that is either soft metal or liquid in a vial. The metal or the vial holds the valve closed. When fire in the room heats the metal to its melting point, or the liquid to its boiling point, it breaks and allows the valve to spring open. Water flows from the pipe and extinguishes the fire. There is also a water flow switch somewhere within the pipe. This switch is usually a small flap, like a pendulum, that moves to the side when water starts flowing through the pipe. Water will only flow if a pipe breaks or a sprinkler has been opened. Sprinklers in hotel rooms may be accidentally tampered with if guests use them to hang their clothes on or otherwise tamper with them. Other causes might be a sprinkler being broken off or freezing and breaking. Water flow alarms, because they are mechanical, are generally not false. It means water is flowing somewhere for some reason and that means trouble.

Manual Switches

A manual switch is most commonly seen at a pull station. A handle or button activates the fire alarm when someone engages it. These may be required by some codes and ordinances and they are very useful for evacuating buildings for reasons other than fires. Kitchen hood suppression systems may employ manual switches as well.

Control Panel

The control panel is really the user interface for the brains of the system. It ties all of the external components together, makes the “decisions” for the system, communicates to other components and the alarm company, and annunciates the activity of the alarm.

When a detector, pull station, or other device is activated, it sends a signal to the control panel. The panel carries out several actions depending on its programming. It will annunciate the alarm (provide some sort of readable signal like a light or buzzer) that tells the type and location of alarm (e.g., "third floor water flow"). It also will activate communication to an alarm company, usually via phone lines, and maybe to other locations throughout the complex (e.g., PBX, Security, and Front Desk). The control panel also activates signals, such as sirens and strobe lights, to warn guests of the alarm. Many larger, more modern systems also have an automatic evacuation message. The brains of the alarm system also make more advanced decisions, such as closing and opening certain air vents, activating automatic door closures, and switching elevators to fire mode.

Many large hotels have a Fire Command Center. Fire Command is a room located in a place convenient to responding fire personnel and away from the mayhem of a fire alarm. This room houses all of the brains and ancillary equipment used for the alarm. Communications panels, public address systems, HVAC (heat, ventilation, and air-conditioning) control panels, and other associated systems are maintained in this room. It is advisable (and often required) that this room is accessible by a "Knox box" or a key to the room held in a locked box that every fire truck has. Fire Command also should be a central meeting point for fire chiefs, security, and facility supervisors, and should contain the following equipment: master keys for offices, guest rooms, and elevators; megaphones, safety vests, flashlights, and other evacuation equipment; architectural plans for the building including structural, electrical, alarm wiring, plumbing, and HVAC; evacuation plans and instructions; a phone and important phone numbers (see Chapter 10, Emergency Planning for more details).

Depending on the size of the hotel, enunciator panels may be located in strategic areas within the complex. A smaller building that does not have a Fire Command Center generally has this panel near the main entrance. If there is a security control room, a panel may be installed there. This expedites the deployment of staff to the location of the alarm without first going to Fire Command. Buildings without such a security room may have a panel at a main reception area, front desk, PBX room, or maintenance control room.

Alert Devices

There are several ways the alarm system tells us there is a fire. That is, after all, the reason for having a fire alarm—to have us evacuate. This used to be accomplished with bells. Now we use bells, sirens, horns, and even lights. Because of excessive noise in some applications and because some people have hearing loss or difficulty, strobe lights are required as well as audible signals. We also now use voice messages to remind people that when an alarm activates, it is better to leave the building. There also may be an "all clear" message when the alarm has been verified to be false.

Suppression

The second objective of a fire system is suppression. Automatic and manual suppression systems are routine and required in most hotels.

Water Sprinklers

Water sprinklers, as mentioned previously, serve the dual role of detection and suppression. Each sprinkler head is connected to the same water supply, but acts independently because it is mechanical. The head is a valve that is held closed by a material that is sensitive to heat. When the heat from a fire rises to that temperature, the material melts (metal) or boils (liquid in glass) and breaks. The valve opens and water flows under high pressure and disperses just like a lawn sprinkler to extinguish the fire. Once open, this water flow does not stop until the entire supply is turned off. In a freezing environment like a parking garage, the water pipes may be filled with pressurized air. When one of these heads breaks, airflow is followed by the water in the pipes from underground or inside the building.

Occasionally, a water-filled sprinkler head may become exposed to freezing temperatures if the weather becomes unexpectedly cold. Just like in a house with exposed plumbing, the head may break as the freezing water expands, and when the temperature warms, the ice melts and water will flow from the broken head. This can be an unexpected mess, avoided by keeping those water pipes above 32°.

Chemical Suppression

There are two types of chemical suppression used in most hotels: those that smother the fire (eliminate the oxygen), and those that alter the chemical reaction of the fire. These systems may be wet foam, dry powder, or gas. They are usually manually controlled, but may be connected to automatic sensors. Although Halon is rarely used anymore, there may be areas in your hotel that use a similar chemical that removes oxygen from a room and is dangerous to humans. Some older systems are under such pressure they can blow out windows, so they are dangerous as well. Be sure your emergency procedures consider these systems to ensure that everyone is safe in the event they are employed.

Standpipes

Standpipes are simply pipes that carry water vertically within a building so that fire fighters can have a water supply on each floor. A wet standpipe is tied into the pressurized internal water system and is ready to supply water when a firefighter connects a hose to it. A dry standpipe is an empty pipe that goes into the building from the outside. The fire department plugs into these at the street level and supplies water to the firefighters on the floor. Dry standpipes have to be used in outside applications and where there is not enough building water pressure.

PANIC ALARMS

Panic alarms are manually activated alarms used to provide an extra layer of security in certain areas of the property. We commonly associate panic alarms with bank robberies and similar events. In the case of a bank or jewelry store, it may be connected to a dialer that communicates a silent alarm to a monitoring station where the police are dispatched. This is the scenario advisable for smaller hotels where there is nobody to monitor the activation of the alarm. (Contrary to popular belief, most police departments will not allow

these alarms to communicate directly with them.) In larger organizations that have a full-time security force, it may be more efficient to have a panic alarm that communicates directly to the Security Department.

Installation

If the infrastructure and size of the property can handle it, panic alarms are best combined with a closed-circuit television (CCTV) system. For example, when a frontdesk clerk is robbed and presses the panic button, cameras automatically engage on the location of that button, bring that view up on a Security monitor, and begin recording that view. Without much more work, other layers can be added as well.

Before installing this type of system, determine what types of threats are to be prevented. Silent panic alarms that will be monitored by an outside company resulting in a police response should be used for robbery and assault only. The idea of a panic button is that it is hidden and used without the assailant's knowledge. Fire panic buttons should be used only for fires, not for medical or other emergencies. Consider the response expected before installing these buttons and training the users on their operation.

Your local police department will not take kindly to continual "false" alarms where they responded to a robbery alarm to find a group of unruly teenagers or a guest with stomach pains.

When a night clerk at a nationally known motel chain was assaulted while on the job, the panic button at her desk did not work. The alarm company knew that the alarm had been broken for four months. The woman, who ultimately escaped the attacker, settled out of court for $2.5 million. Security equipment that does not work is not only useless, but also provides a false sense of security. Regular inspections will not only ensure that the equipment is working, but also will provide a good defense against lawsuits like this.

Silent alarm switches should be hidden in a place where they are easy enough to access, but not where they will be activated accidentally. The switch can be the best accident avoidance just by its design. Some require a two-finger pinch or a hole where the finger has to be inserted. These cannot be depressed with a knee bump if under a desk. Another idea for a cash drawer is a bait clip or "mousetrap" switch. The two leads on this type of switch are separated by money within the till. When the money is pulled during a robbery, the two leads touch and cause the alarm. There are also foot switches, pull cords, and just about anything that can be a switch. If the purpose of the alarm is a medical emergency or something where its activation will not jeopardize the safety of the user, it can be mounted on a wall, desk, or just about anywhere. The more visible this type of switch is the better.

Associated Equipment

Camera operation during an alarm is also dependent on what will be the reason for the alarm switched to be pressed. Several cameras may be needed to cover the area where

the alarm is tripped, the egress points of the area, and an overview. In the old days, the cameras in a bank were film recorders so they would not even record at all until the switch or bait money was pulled. Then every camera in the bank would begin recording. Now, with digital recording and cheaper cameras, we can use the same concept, but instead of starting the recording, the switch might cause movable (PTZ: pan, tilt, and zoom) cameras to turn and zoom into those certain areas. For example, suppose you have four cameras covering overview shots of your main lobby. When a panic button is depressed, one camera zooms in on the main doors, another on the elevators, and one on each side of the front desk to get opposing shots of the incident.

Camera "salvos" like these are dependent on your camera types and their interface with your alarms. If you have someone monitoring video all the time, this modified view of the emergency can assist deployment of security staff or even allow someone to phone the police with an update of the situation. Some companies use the panic button to activate other hardware besides cameras. You can connect lights that alert other persons, lock or unlock certain doors, activate safety shields, and so forth. The possibilities are endless.

Operation

Training on the use of these panic buttons is critical. As mentioned before, the police tend to assume silent alarms are robberies in progress. If your employee uses it for someone with a counterfeit bill or a bad check, the police are going to scold you for crying wolf and may even levy fines. The opposite is also true. If an employee hits the medical emergency button for a man with a gun, medical personnel and unarmed security may come running into an unsafe situation. I suggest testing these alarms on a monthly basis. Make sure it communicates properly (after telling the communications center first) and that cameras and other equipment tied to the alarm work properly. Use this testing as an opportunity to reinforce training. Have the users push the button so they know how to do it and ask them under what conditions they would press it. One minute of training could save lives.

INTRUSION ALARMS

Intrusion (or burglar) alarms are very different from robbery or panic alarms. The main difference is that a burglar alarm is automatic, being activated by the actions of an intruder. The panic alarm is activated by an employee or victim of a robbery. Intrusion alarms use several different types of switches or sensors to activate the alarm. Then that activation is sent to a communications center for police dispatch or to the in-house monitoring area. In some cases, burglar alarms are "local," which means they do not communicate at all and just activate a bell, light, or even a camera.

You may think we do not need burglar alarms because hotels never close. However, there may be some areas that need to be secured even when the facility is open, such as store rooms, and some areas that are restricted at night, such as offices or kitchen areas. So, consider these methods of using alarms to keep your hotel secure and possibly reduce the amount of Security staff.

The first component of a burglar, or intrusion, alarm is the switch. The most common switch is the magnet switch or contact switch used on doors or windows. It is simple: bad guy opens the door or breaks the window and circuit is broken causing the alarm. Next most popular is a motion detector. These can be infrared, photoelectric, or any of several more complicated technologies. These very versatile devices can be used easily to detect persons in a kitchen or convention area. Your Facilities Department may already use these types of devices to monitor climate, boiler pressure, and other comfort and critical systems.

Main Processor

As with a fire alarm, we need a brain to gather information from these systems and decide what to do with the signals. It may communicate to a dialer that notifies the alarm company for police dispatch or your monitoring facility on property. It also may activate a bell, siren, light, camera, or other alerting device. Even cell phones can be the receiver of an alarm.

Most digital camera systems also conduct motion sensing and intrusion functions. These are discussed in the CCTV section of this chapter.

Monitoring

The final component of an intrusion system is the monitoring station. If it is a security facility, then it will be tied in with the design of the control center with procedures for responding to such alarms. A smaller hotel may utilize the frontdesk clerks, who are usually the only people awake all night. They can have a panel that tells them when someone is entering the closed pool, the closed meeting rooms, or breaking into the arcade games. Once again, the possibilities are endless and a little creativity will eliminate some of the need for human patrol during certain hours.

OTHER MONITORING SYSTEMS

Security is often tasked with monitoring many other systems besides Fire and Intrusion. Either this is because of their relevance to Safety or because Security is the department best equipped with a monitoring facility.

Some systems requiring monitoring in a hotel are elevators, escalators, water boilers, generators, valves, HVAC systems, and pool equipment. Many of these systems used to require a human to babysit them and ensure that the machinery did not malfunction, overheat, or cause some sort of safety hazard. Technology has allowed us to watch these components of our hotel remotely and thereby with fewer humans. For example, many hotels still in existence today require an engineer to watch water boilers to ensure that they do not leak or overheat, resulting in an explosion. Modern boilers are built a little safer and with sensors that can be monitored remotely. It is a much more efficient use of time and resources to allow one person, whether it is a security officer or engineer, to monitor all of the systems from one control room. If you have such a control room for video monitoring, dispatching, or alarm monitoring, consider using cameras or sensors to watch some of these important nonsecurity functions.

ACCESS CONTROL

Access control is one of the main functions of Security Departments everywhere. This goes to the very infancy of our industry where asset protection was best accomplished by controlling access. Access control includes locks on doors, remote switches that open locks, officers watching doors, and electronic access systems.

Most hotels now employ some sort of access control system on their guest rooms. Still, more facilities fortify their security with access control to their restricted areas, elevators, and offices. The concept of electronically controlled access requires a reader, an authorization, a mechanism, and, of course, a procedure.

Reader

There are many types of readers and technology is constantly finding ways to make them stronger and more convenient. The reader in its most primitive form is the tumbler or pins within a lock. A key is inserted and the pins are arranged by the key into a unique configuration that allows the cylinder to rotate. The weakest part of this system became the key, which is easily duplicated, lost, or broken.

The next basic reader was a magnetic strip. This method works just like a credit card reader. A card with a strip is inserted into a slot and a magnetic head reads the code from the strip and activates a solenoid or a motor to open the lock. This system still prevalent in hotels has a few faults. The magnetic strip can become worn or demagnetized, the codes can easily be read and duplicated, and the card can break or get lost. Few systems use a bar code in the exact same way as the magnetic strip. These are very easy to duplicate.

Radio frequency (RF) chips are a bit newer than magnetic cards and slightly more secure. An RFID tag is embedded into a card or other object. The lock produces a radio signal that bounces off the RFID tag and receives its data or code. The code is the key that opens the lock. RF locks are a little more expensive, but also more difficult to hack. However, technology is advancing very rapidly that can read these tags from a short distance and obtain their coded information for duplication.

A technology that is really exploding turns the human body into a key. Biometrics allows the reader to read unique features of our anatomy as a key to open a lock. Patterns in the human eye, fingerprints, voice, and now vascular systems are some of the ways we use humans to open doors. This technology is becoming more prevalent and less expensive and is, thus far, almost impossible to circumvent.

Authorization

The second part of the lock is the portion that allows the lock to be opened. In a pin and tumbler lock, it would be the pins. The key puts the tumblers into a certain position and the pins have to align and allow the cylinder to be turned.

In a magnetic or barcode reader, the authorization is in one of two forms. A standalone lock, such as older hotel locks, may have a list of authorized codes that allows entry. The guest key code might be 1234, the housekeeper code might be 2234, and the manager

master code might be 9234. Each code will work because it is on the list in the memory of the lock. The different codes allow for different levels of access and for identification of which key was used.

In an integrated system, such as one that uses a computer to control several locks in a building, the reader transmits the code to the computer for verification. The computer has a database of authorized persons and the corresponding code allows the door to be opened.

RF keys work in a similar manner. The lock reads the code from the tag and compares it with its internal memory or through a wired system that reads a database.

In biometrics, the reader turns the anatomical pattern into a numerical value called an algorithm. The algorithm converts to a simple integer and compares with a database just as above.

Mechanism

Mechanisms that open locks have little to do with the reader. Thus, a magnetic reader may be used with a motorized lock and a biometric reader may be used with a solenoid lock and vice versa.

In a motorized lock, once the reader authorizes entry, a switch or relay is opened allowing electrical current to flow to a motor, which turns a gear, which slides the latch open. This motor also has to close the latch after entry.

A solenoid lock allows current to flow to a solenoid (kind of an electric spring), which moves a pin or bolt that allows the latch to be turned manually. (A solenoid is the device on a pinball machine that kicks the ball back into the field when struck.)

Motors and solenoids are sometimes used in combination in various types of locks.

As you have probably experienced, these components of a lock do not have to be inside the lock. The reader may be mounted on a wall, the computer may be in a closet, and the mechanism embedded in the doorframe.

Remember that a lock is just one layer of security and should not be expected to be impenetrable. Each type of lock can be defeated electronically or mechanically with simple tools and skills.

KEY CONTROL

One of the responsibilities of the Security Director is key control. Whether you have electronic access control, metal keys, or a combination of both, the accountability for these systems is paramount. We will go over the basic and various components of the two systems and the proper accountability methods that you can customize for your property.

Access Levels

Key systems consist of a hierarchy of access levels that are generally classified as individual, group or submaster, master, and grand master. The hotel may have different names for these levels like room, floor, section, zone, and master or emergency. Do not worry if you are missing a level or have some extra levels. That is not important right now.

Access to a particular level or group of locks is based on job necessity. A maid, who is cleaning rooms on one floor, does not need a key that fits every room in the building. Just like the Marketing Director does not need a key to the accounting office. Therefore, we issue keys and group locks by user instead of by location. Most electronic systems will allow you to program a key to fit just those rooms you need. Older systems group the rooms and keys by floor. Key locks for your offices are by department.

The grouping of keys needs to be in some order before the master keying of a property can be done. Not as important for magnetic locks is the tumbler configuration in a key lock. Your locksmith can explain this better than I can, but pins of different lengths are aligned to allow a cylinder to turn when a key is inserted. To allow a submaster and a grand master to work on this lock, another level of pins is utilized within the cylinder. Therefore, to configure the pins for the unique key, the locksmith will need to know which group or submaster is going to also be used for this lock.

In a hotel, we generally group locks by department. All the administrative offices may be one group, the maintenance storage rooms another group, and perimeter doors another. When the locksmith is keying each of those locks, he or she will also configure the pins for the group master and, of course, the grand master.

Group masters or submasters are those keys that fit more than one lock in a group. Management sometimes is carried away with this system and gives everyone in a department a group master so they will not have to carry so many keys. If the convention sales coordinator needs a key to his office and a key to the supply storage room, give him those two keys. Giving him a key to the entire sales group is a waste and gives him access to areas he does not need. What is the big deal with this if we trust him? Plenty. If he loses his group master, you will have to rekey locks on every door in the group and reissue keys to everyone in that group. Moreover, if something comes up missing from one of those offices or storerooms, now you have more suspects to consider.

The only one who needs a group master is the one who needs access to every door in that group. That is not necessarily the boss, although he or she will want one. Perhaps it is the secretary or the person responsible for inventory. It is very important that keys be issued and accounted for by one person or department, such as Security. There should be a process in hiring, firing, and transfers that ensures only current employees have access to their specific areas. What tends to happen is, employees come and go and they may forget to turn in their keys, or only turn in some of them because they put their office key with their house key and they forget about it. When that loss occurs, you don't know who the suspects are because there are unknown keys in circulation. Worse, a termed employee turns violent and now we don't know who has access to the new boss's office. If we have an accounting of who has which keys at any given time, the necessity and expense of changing locks becomes moot.

Grand Masters

Grand master keys—those that fit every lock in the building—are usually not taken as seriously as they should be. Everyone wants one as a matter of prestige. The General Manager wants one, the CFO wants one; in fact, most department heads will justify their need for one in case they are working late in the office or showing clients and vendors around. This

is a huge liability and you need to put your foot down on this one. None of these people needs a key to every single door in the property. Maybe a submaster will do. Explain to them the cost of rekeying every lock when they lose theirs. Explain to them that they will have to be investigated like everyone else who has a key when property comes up missing. Tell them they will have to justify their whereabouts if a witness reports two people having sex in a linen closet after business hours.

Grand master keys should be limited to those that need emergency access to every part of the building at all hours. Ideally, it is checked out as needed and never leaves the property. There needs to be one or more available for fire department and SWAT team personnel and that is about it. If someone needs to get into the controller's office because he is away on vacation, then he or she can call Security.

If you are fortunate enough to key or rekey your building from scratch, keep these considerations in mind. Do some research on quality locks. Endurance of the parts is more important than the unique key configurations. If you are replacing hundreds or thousands of locks, go with a company that will provide a unique key profile (one that is hard to find at the local hardware store). Remember that a lock will not keep out criminals. Locks are a deterrent to unauthorized entry, so they really just keep people honest. If you are trying to secure a room against entry, you need multiple layers such as cameras, alarms, and other locks. Establish a numbering and filing system for keys and their users. This system should be based on the grouping we discussed previously. Finally, make sure strong and thorough policies are in place to protect the integrity of your lock system: duplication of keys, reporting lost keys, turning in keys upon termination, unauthorized use and trading of keys, etc.

CCTV

Closed circuit television is really an outdated term, but it is technically an accurate way to describe video systems. Video systems have changed dramatically over the past 20 years, with the most drastic innovation being digital. The main components of a video system are the camera (input), a switch (control), a recording medium (output), and a monitor (output).

Cameras

Even if we have not been intimately involved in their operation, we have all seen how cameras have progressed over the years. Of course, like everything else, they are smaller, but they also have improved in color, clarity or resolution, and image type (digital versus analog).

Analog cameras are still very much in use, but they are slowly being phased out. Analog cameras are the ones you have in your facility if it is more than five years old. Without getting too deep into the technical stuff, analog is the format delivered through the modulation and amplitude of linear frequencies. The bandwidth used to deliver the image does not change, so storage and resolution do not really change.

For analog cameras to record their image onto a digital recorder, such as a DVR, their signal needs to be converted to a digital format. This is often through an external piece of hardware installed somewhere between the camera and the DVR or in the DVR itself.

Digital cameras convert images to data instead of frequency and amplitude. Therefore, the image does not degrade through copying or transmission. Either it makes it or it does not. Analog television that has interference gets shadows, wavy lines, and distorted images. Digital television has the same clarity regardless of the interference. The interrupted pixels are just taken out, resulting in a blocky image.

Camera installation depends on the application and the purpose of the camera. Fixed cameras—those that do not remotely move or adjust—are used to watch a single two-dimensional rectangle image. If everything that needs to be viewed is within that rectangle, then a fixed camera is the way to go. Different lenses and add-ons can be used for wide angle, telephoto, and low light conditions. Remotely operated or automatically moving cameras, called PTZ have motors in them that move the camera side to side, up and down, and in and out. Side to side is actually a rotating function, turning the base of the camera any place within a complete circle. Tilt refers to pivoting the camera on its base and zoom is controlled by the lens motor like a consumer camera. The focus and iris generally have a motor to keep objects in focus and the light balanced as the camera moves. These moving cameras cost about 10 times that of a fixed camera, so you need to justify their installation.

A PTZ camera really has more than a 360-degree field of view. Think of a camera mounted on a ceiling. It can rotate 360 degrees around in a circle. It also can tilt from the horizontal view of the ceiling all the way down to a vertical view of the floor. This is 90 degrees of tilt, but because the camera can rotate around, the camera sees 90 degrees back up the opposite side. In other words, if the camera were mounted inside of a globe, it could see the entire southern hemisphere of that globe.

PTZ cameras are used in two applications. First, they can be programmed to automatically "patrol" any area within their 360- × 180-degree field of view. Whereas they used to just "pan" from side to side, now we can build a "macro" that rotates, tilts, and zooms the camera all over the field of view. This is common in a large area like a parking lot where the camera patrols the outer perimeter, then angles down to each lane of the lot as it tours the entire area.

In reality, these cameras, depending on how long their tour is, will miss many of the important incidents you are trying to capture. While the camera is looking at one side of the lot, the crime could be occurring on the opposite side. However, the deterrent is there, and if the camera is concealed in a dark housing, the bad guys will not know where it is looking. The automatic camera also provides some other investigative tools, such as "time-framing." If you are looking to see when an incident happened, such as a broken window, you can narrow it down to the time of the camera tour by reviewing the video.

The second application for a PTZ camera is where monitoring takes place live. Casinos regularly use PTZ cameras to view the action on table games or to follow subjects around their property.

A third type of camera is fixed but also allows for the features of a PTZ. These cameras are referred to by many names, brands, and technologies, and produce a 360-degree image all at once. Imagine your favorite Internet map site. You can go to street level and look at a view of your neighborhood in a 360-degree circle. This is done by a car driving on your street with four (usually) cameras that have a 90-degree field of vision. The cameras are in time sync and software within "stitches" the four images together so it seems like it is one image. Another method of doing this is a special lens that is like a "fisheye," but produces

Most nonsecurity managers will turn to cameras to solve their crime problems. Meat is missing from the freezer—put up a camera. Employees are having sex in a closet—install a camera. Graffiti is found in the parking lot—buy another camera. It is important to remind these managers that a camera is not the answer. You will not catch a crime in progress with a camera unless you have the workforce to monitor it live. Even if you get a video image of the suspect, you may not be able to identify him or her. Even if you identify the suspect, you would have to get police to file charges and go after him or her. After all that, recovering the loss is unlikely.

Cameras are a good deterrent because most criminals are hesitant to commit a crime on video. Some companies take this to the extreme of installing dummy cameras that do not work. Most lawyers will advise you against this as it provides a false sense of security if someone is being assaulted and is relying on these cameras to catch the act in progress.

the same hemispherical image with one camera. So, when monitoring the same parking lot, instead of moving the camera, you just increase the magnification of the area of the lot you want to see. This is like a virtual PTZ because the entire range of the camera is available for view; you are just moving your view of that image. These cameras eliminate the missed images from the auto pan camera and they are coming down in price because they do not need the motors used in a PTZ.

Camera Mounting

The standard practice for mounting cameras has generally been on the ceiling or high up on a wall. This prevents tampering, blocking, and generally provides a good overview of the area. In some situations, this may not be the best practice. If the purpose of the camera is for facial recognition or to get a good view of a subject's face, being high up is now one of the worst locations. Most bad guys tend to look down so people will not see their faces and they wear hoods and caps that mask them from high cameras. License plates on cars also are not read very well from a high angle. These need to be viewed from plate level. The good news is that cameras are now smaller, easier to conceal or put out of the way, and can be made to be tamper resistant. Many teller windows in banks and retail now have cameras affixed to the counter. The camera gets a facial view of the customer. Even if he does not want his face seen, by the time he notices the camera and blocks it, we already have his image. You also can mount a camera in a tamper-resistant bubble right at eye level near a doorway or at an intersection in a crowded lobby. By the time most people see it, it is too late to avoid it. Even if they do know it is there, it is a great deterrent, like the greeter at a retail store. Cameras can provide a very good image from a very small hole, so cameras can be mounted in walls, cabinets, fixtures, door frames, and just about anywhere else.

Covert cameras can be very revealing, but can get you into trouble if used in the wrong setting or for the wrong purpose. Generally, you should not put a camera in a place where someone has an expectation of privacy. Bathrooms, locker rooms, and guest rooms are big no-nos. Even offices may be trouble if they are considered private. Audio recording laws

vary by state, but generally do not permit recording unless notice is given. Check with your lawyer for these applications.

The bottom line on mounting cameras: Decide what it is you are trying to view, the best angle from which to view it, and then figure a way to get the camera to mount in that place.

The Switch

There are many different names and configurations for the hardware that controls the cameras and routes their signals to recorders and monitors. Commonly referred to as a switch, this device or set of devices acts like a phone switchboard and takes the input of the camera signal, marries it with the remote controls for the camera, and assigns the signals to the outputs: the recorders and the monitors.

The switch allows you to have more than one remote controller within the system. The security control room will have one, but the hotel manager may want one of his own. This is not difficult to install, but you must ensure that the security controller can override the others in the event of an emergency or important investigation.

Many newer systems have a "virtual" switch. In this situation, all the cameras go into the computer and the software assigns them to various monitors and recorders and provides remote controls.

Monitors

Video monitors in analog systems are installed parallel to the recorders. The video signal comes from the switch and is split between the monitor and the recorder. The monitor is viewing exactly what the recorder is recording. In a digital system or one with a virtual switch, the monitor is viewing whatever the software sends to it. So, while the recorder is recording live, real-time images, the monitor can be used to watch other cameras, playback of recorded material, or enhanced and multiple images created by the software.

In older configurations, we would use one monitor to watch one camera view, or split views of two or more cameras. The cameras assigned to the monitors could be changed, but that created confusion when reviewing playback. With a software system, any configuration of views can be displayed and changed without affecting recording or playback.

Therefore, configuration of monitors (what we want to watch live) is dependent on who is watching, what is being watched, and what the purpose of watching it is. We need to know who is watching it because a hotel manager is looking at his employees goofing off, if there are long lines in his lobby or valet, and other business-related functions. The chief engineer wants to see that his equipment is running properly and nobody is tampering with it. These are self-explanatory configurations and their monitor setup will not affect the security of the building.

The security monitor setup is much more important. Before we look at the physical setup, we need to tend to the human aspect of watching video. Most studies have shown that a person cannot effectively watch more than about 10 monitors. Even at 10, there is fatigue that occurs after some time and is dependent on other duties, such as dispatching and logging of activity. It also depends on what is being watched. A person trying to watch 10 images with a lot of activity will not see everything he should. If he is just watching 10

doors to see if someone enters them, then that would be easier. To have the most effective video monitoring station, set it up something like the following:

Create a video wall of monitors on a vertical surface in front of the operator. Three-sided viewing stations or curved walls cause blind spots and fatigue from the officer moving his head around. This wall will use peripheral as well as direct eyesight. The distance of the wall from the operator depends on the width of the wall. If the wall is wide, it needs to be farther back or vice versa. Keep the distances short enough so the operator will hardly move his head, but just move his eyes from one side to the other.

Those images that have less activity are placed near the outer edges of the wall. They can be of a smaller size because we are not looking for detail, just movement: a back door of the hotel, the company safe, the receiving dock at night. Near the center of the field of view (eye level) should be the larger monitors showing important areas of activity: the main lobby, the pool, nightclub, retail center. At desktop level, right in front of the operator, are two or three working monitors. These cameras may show alarm views, and will be used for patrol. These also can be used to bring up images seen on the smaller monitors that require an extra look. (This was discussed in Chapter 8.)

Recorders

Once again, back in the old days, we used videocassette recorders. We started with one recorder recording one camera, and many older buildings still employ this type of system. In the late 1980s, we advanced to multiple recordings of cameras onto one tape. These multi-recorders took an input of (up to) 16 cameras, recorded a frame from each of them every second, and recorded it on the tape. Using the same machine to play back the images, we saw one frame of video per second. This created a choppy image (TV is about 30 frames per second) and was useless for watching currency transactions, but acceptable for watching closed areas for activity. The advantage was using one video cassette instead of 16. Digital video recorders (DVRs) came on the scene in the late 1990s and made this process much better. The frame rate on a DVR can be adjusted from 1 to 30 so the clarity of the image is improved. Also improving the image is digital recording instead of analog. Because each pixel from the camera is duplicated onto the recorder as data, there is little or no loss of clarity. Finally, compression has allowed us to save storage space on the DVR with less loss of picture.

If you are like me, you care less about how the DVR does its job and more about *if* it does it. Here are the basics you need to know when selecting a DVR configuration.

Frame rate is from 1 (choppy) to 30 (smooth). Thirty frames per second is better, of course, but uses way more storage space. And, it is really not needed. A view of a door or gate can be at a lower frame rate because the movement is less important. A camera view of a poker game requires a higher frame rate to see the cards, the action of the deal, and the money exchanging hands.

Number of ports only matters in the event of a failure. If you lose the DVR or the hard drive crashes, you lose all of those camera feeds. There are different types of backups or even redundant systems that should be employed in case a unit fails or even becomes full.

Storage space is now relatively small and inexpensive. The problem is that as we get storage space more compact, we also get better camera resolution, which uses more storage space. You just need to watch as you increase resolution that you have your storage limits increased proportionately. Over 30 days is probably not necessary and most hotels find that 7 to 10 days of storage is acceptable. Remember that panning cameras and those with more motion use much more storage than fixed cameras with no activity. This is not due to frame rate, but compression.

Other recording systems are still digital but may be computer- or server-based. These record as a DVR does, but store the data on servers that are linked. When one server is full, it switches to the next, and so forth. One or more servers can be used as a backup and either simultaneously store data or begin storing when another fails. This system is called a network video recorder (NVR).

REPORTING SOFTWARE

The second most important job of a Security Department is documentation. (Prevention is first.) All activities of the Security Department must be documented to show evidence that those events occurred, how they occurred, and why they occurred. Daily logs of patrol activities and incident reports of unusual events are the most common and most important of the events that we document. Logs are used to research incidents, show evidence of preventative patrol, and track performance of officers. Incident reports provide a summary of an event to upper management, present our side of the story of an incident in court, and track events for later risk assessments.

The traditional way to document activity is a paper log. A standard table or spreadsheet of date/time, location, officer, and activity is the general structure of this log. Incident reports generally consist of a fact sheet with the statistics of the event and those involved, a narrative, supporting statements, and summary of evidence. (Report writing is covered in Chapter 11.)

Since the personal computer became prevalent in business, we have turned to the word processor to write our reports. The software does not matter—as far as the final product is concerned—because our legal system still uses paper documents. Thus, the selection of using pen and paper, word processor, or reporting software really does not matter from a legal standpoint. This is a business choice and is dependent on the convenience of the users.

In the past 20 years, software companies have produced reporting software specifically for the functions of security. This type of software generally integrates several modules, such as daily logs, incident reports, Lost and Found, personnel management, and others. There are three big advantages of using this software over the standard word processor.

Searching is one advantage of reporting software. Looking up a previous incident by a guest's name or date becomes much easier and faster. Another advantage is statistical data reports. You can determine crime trends, costs of incident management, total losses incurred, and whatever is important to you. An archive is the final advantage of reporting software. Data obviously saves room over paper documents, but is also safer because it can be backed up and filed in different ways.

Because reporting software does not really improve the quality of the final product, your decision to purchase and use it will depend on whether it saves you time and money. A smaller hotel may not save very much time on reports and logs in this type of system, but a large hotel that produces massive amounts of data will find that an integrated system will save time and labor on inputting data and exporting it.

TRACKING SYSTEMS

The justification for tracking systems was discussed in Chapter 8. The tracking system takes the place of manually logging the patrol routes and frequencies of our officers. Instead of relying on the integrity of these logs and the inherent "fudge factor," the tracking system proves that our officer was where we said he was. This section discusses the tracker's technical aspects and how they are operated.

History

Tracking systems date back to the middle of the last century when night watchmen would tour a building. They wore a large clock on a strap around their neck and each time they came to a designated check station, there would be a key hanging there. They would insert the key in their lock and it would log that they were there at that time and place. Over the years, the concept has hardly changed and the two components have only changed in their size and technology. As you might imagine, our biggest challenge is the human component that seeks to defeat the system, which feels like they are carrying around their own supervisor.

Today

Sixty years or so has taken us from keys to magnets to magnetic encoding to barcodes and radio frequency. Most devices now use an RF chip that is read by a handheld reader the size of a couple of rolls of quarters. The RF chips or buttons are placed in those strategic places around the property that you want inspected on a regular interval. Hotel stairwells and linen rooms are common hotel patrol points. Boiler rooms, swimming pools, laundry rooms, and kitchens might be other applications.

Buttons

The buttons are placed with glue or screwed into mounting plates and then the location has to be logged into a database. Buttons can be as small as a dime or as large as a cigarette lighter depending on the type of reader, but should be mounted out of the way and in an inconspicuous spot where the decor of the area will not be compromised. Be aware that the location of and around this button will become worn and unsightly. Constant contact from hands, fingers, the reader, and so forth tends to wear out wallpaper, paint, and polished surfaces. It is best to hide it. The officers will know where it is and guests do not need to see it. Buttons will wear out over time and often become dislodged from the surface. This is to be expected.

The Reader

The reader is a device usually carried in the hand and may be used with a belt holster, a wrist strap, or carried in the pocket. Lately these devices have been made out of metal, as the plastic ones tend to break with abuse. I have seen these things abused like you cannot imagine. Security officers, regardless of how the trackers are justified as their "friend," absolutely hate carrying them. I suppose they see them as babysitters or supervisors always looking over their shoulder. I have caught officers beating them against the wall, throwing them off the building, dipping them in water, and even trying to electrify them. This piece of valuable equipment, like a car or radio, needs to be inspected at every changeover and those in possession of it held accountable for damage.

The reader, usually referred to by its brand name, reads, collects, and stores data from the buttons. The user touches or scans the button and is rewarded with a beep or a light. The data is stored in memory until downloaded.

More advanced readers are actually wireless GPS transmitters that send the data via an internal network. This is a great safety device, for location of the officer, if you can afford it. A cellular device with GPS is not practical for hotels because of their vertical locations. These are better used for wide area patrol. Some buildings have been equipped with an internal GPS or locator system. It uses internally installed transceivers to pin-point locations. This system can be integrated into your radios, phones, track readers, and dispatching system as one system. Imagine the benefits of knowing the location of your employees at all times.

Tracking Software

The reader, unless it transmits wirelessly, needs to be downloaded on a regular basis to a database. I recommend doing this every time the reader changes hands. This gives an opportunity to inspect the reader and save its data before it is accidentally lost.

Once the data is downloaded, the reporting software allows management to review the activities of its patrol officers. Never assume that patrol is going along fine without checking. Lazy officers will test you by not using it or using it incorrectly. Supervisors need to address gaps and inconsistent patrols on a regular basis.

Management will need to decide how many buttons need to be "hit" in a patrol route and how long the gaps between buttons can be. If you require one tour of your tower every hour and there are 20 buttons, then there should be no more than three minutes between hits and all 20 buttons hit. There will be exceptions if an officer has a noise complaint or a report in a guest room. This is an acceptable gap, but should be logged to explain the gap later. Some suppliers provide a wallet with "excuse" buttons for the officer to scan if he goes on a call. These scans in the data report can be matched with the dispatch log to make sure the officer is not abusing the process.

As mentioned in the Chapter 8, this tracking system can be your best friend. When the unthinkable happens in your hotel, this proof of your preventative patrol may be the only thing that saves you from an inadequate security ruling.

LOST AND FOUND

Lost and Found policies are discussed in Chapter 8. This section explores the systems used to manage the Lost and Found process. Many reporting software products offer a module that helps to log items left unattended by guests. Because we are unfortunately responsible for these items left in our possession, we protect these assets as if they were our own. Like our other logs and reports, we can do this with paper, a simple spreadsheet, or a commercially produced software program.

Unlike reporting software, the Lost and Found database needs to have some security functions. A simple spreadsheet would be difficult to secure so that other users could not delete entries or edit them. When creating a program—or purchasing one—keep the following features in mind.

Access Rights

Users of the property database need to have access rights depending on their duties. Be careful not to give any one person the ability to enter, modify, and return items. There needs to be a check and balance or dual security on these transactions to avoid theft.

Audit Trail

The software should include the ability to track every data entry, modification, or deletion. The report should include the date, time, user, and action taken. This will be a way for management to audit the integrity of the users and the process.

User Access

The system should be server-based so that the database can be accessed from various locations on the property. This is for guest service.

EMPLOYEE LOCKERS

Lockers naturally fall under the purview of Security because they provide asset protection. Many businesses buy lockers, install them, and let the employees use them as they please. These days, you need to regulate and administer lockers so they are not abused, used for criminal activity, or prone to be a nuisance for the company.

Lockers

Locks on the lockers need to be of a type where management can open them. Keyed padlocks with a master key are probably best. Combinations are too complicated for many employees and are difficult to track and change. Make sure the lockers are in open areas where theft can be kept to a minimum.

Locker Placement

Locker rooms should be avoided because you cannot install cameras and thefts are more likely where employees forget to lock them. These lockers tend to become health hazards with dirty clothes, old food, and other live-out-of-the-locker issues. Lockers are best placed in hallways where there is traffic to watch them. Encourage employees to take their items to the dressing room for changing. A public area naturally discourages employees from leaving their personal items, trash, hangars, etc., around their lockers.

Security for Lockers

You cannot place cameras in a locker room, but if they are in a hallway, cameras used for watching other areas can watch the lockers as well. Theft most commonly occurs when employees forget to lock their lockers, or when they are too lazy to lock them. Make this part of your back-of-house patrol to check lockers and locks. Employees who steal from fellow employees are about as low as you can get. Anything you can do to prevent or catch these thieves is best for your property.

Problem: Employees leaving lockers unlocked in the men's locker room find their property stolen during their shift. Solution: You cannot put cameras in a men's locker room—or can you? How about a hidden camera inside a locker? Set up a camera that just sees the face of the person opening the locker and nothing else. Place some bait in the locker and wait. Anyone opening the locker is a likely suspect and if you cannot see them remove the item, that is okay because you know they are the only ones who opened it. Remember, we do not need evidence or all of the elements of a crime to terminate an employee for stealing. This is an easily justifiable termination and you never have to reveal to the suspect that you had a camera there.

KEY DISPENSERS

Key dispensers used to be security officers. It did not take long, after these automated devices were created, to justify them through labor savings. A key dispenser is generally a cabinet that securely holds several key rings until they are individually unlocked from the cabinet electronically. The access method can be a numeric code, print reader, magnetic swipe, or any type of access device you want to attach to it. Key dispensers can issue keys without having another human present, or they can require two or three people to be present (to enter their access code) to issue a high security key set.

Key sets used in key dispensers are of the type that cannot be opened without damaging the ring, so one of the keys cannot be removed without authorization. In fact, this type of ring should be used for all issued key sets, whether or not you use the dispenser.

The most wonderful thing about the key dispenser—okay, the second most wonderful next to labor savings—is that it keeps a permanent audit trail of keys issued. In fact, you can set alarms so that high security keys kept out past their curfew notify you so you can

see what is going on. Key dispensers are expensive, but if you spend a lot of time issuing keys, looking for them when lost, or figuring out who has what and for how long, they may be for you. Key dispensers also can be modified to issue other items, such as radios, patrol track wands, etc.