Unit 17

Crisis Management in an Organization

Learning Outcomes

By the end of this unit the learner will be able to:

- ✓ Understand the main objectives of a security framework and how to achieve them
- ✓ Explain how technology is having a positive effect on security standards
- ✓ Describe the potential limitations of a technology-heavy security system

Unit 17

Crisis Management in an Organization

Security Goals

The general goals of physical security are to control access, prevent the interruption of the organization's mission, and eliminate or reduce theft and losses. Regardless of the size of a facility in total acreage, number of buildings—whether one-story or multi-story—the security planner must first conduct an in depth study of the entire facility and determine the needs when approaching and planning a security program. This effort should take into account the goals of the organization as they relate to security, geographic issues or constraints, and the type of general and specific protection that is desired, within budgetary limitations.

These goals are accomplished using tangible countermeasures (ranging from fencing and lighting to electronic surveillance equipment,) paired with carefully defined policies, procedures and event reporting systems. Security programs, because they cost money, must be judiciously planned in order that the greatest return may be obtained for the money spent.

While facility and security managers are concerned with the general organization goals, they may also have immediate specific goals, such as those discussed below:

- ensure adherence to building codes and safety requirements
- improving relations with local law enforcement
- hardening buildings against structural damage
- boosting employee knowledge of security issues
- building wider stairwells for evacuation
- enhancing brand image with more effective security
- improving fireproofing
- creating building evacuation plans
- installing backup emergency lighting

Technology in the Field of Security

The physical security component is focused on obstacles and barriers. This is the application of barricades, fencing, gates, and walls, outside perimeter lighting, signage, and locks. Operational security involves people. Specific issues include the provision of staff to support the security protocol, the education and training of employees, and procedures for managing contractors, vendors, and visitors.

The third component is **technological security**. This involves the management of technical data and systems. It includes the integration of video surveillance monitoring systems, alarm systems for intrusion detection, building automation systems that control HVAC and lighting, fire alarm systems, communications systems such as FM radios and emergency call boxes, and access control of space. Complex and costly parts of the plan may be prioritized for implementation in the future.

The introduction and use of technology represents one of the most important steps in the development of an effective security framework, alongside training, policy implementation and regular reviews:

- **Security Training**. Training will elevate security awareness among all employees. It should include employee familiarity with the plan and use of the installed security equipment for conducting data and information analyses. Security and facilities personnel should be trained in how to diagnose and respond to facility threats. Responding to a threat must be practiced. If it is not, then the plan is just another document sitting on the shelf, gathering dust.

- **Use of Technology**. Determine which technology is best to support the requirement at hand. Doing this requires an understanding of the risk. Consideration must be given to the organization's mission, crime in various geographic and demographic locations, previous security issues, and current conditions.

- **Policies and Procedures.** Good policies and procedures must be understood by everyone and interpreted in the same manner. All employees, building occupants, vendors and contractors, and visitors should be provided with a copy of detailed procedures to follow in the event of a security or emergency situation.

- **Review and Revise**. Emphasize the chief executive's support for the plan, schedule regular reviews, and solicit feedback. It is important that this be done within the first ninety days of implementation. If employees know that support exists at the highest level of the organization and that plans will be reviewed regularly, then those individuals and groups responsible for implementation will take greater interest in ensuring that details are well coordinated. Consider having a performance measure for security compliance included in employee reviews. Feedback and recommendations from employees are also important in order to assure their cooperation.

The Growing Importance of Technology in Security

Manpower continues to play the single most important role in the security frameworks of most businesses worldwide. However, we now live in an era where to effectively safeguard an organization and its assets *without* technology would be unthinkable.

The last two or three decades in particular have radically altered the way the world has come to depend on technology. Along with paving the way for sophisticated security systems that were never previously possible, technology also lightens the load carried by security personnel at all levels. Manpower will always be required, but sophisticated security technology can make it much easier to protect premises and personnel from harm.

Technology can be used to achieve almost anything, though in the field of security supports the two primary components of a wider security framework - **access control** and **surveillance**.

Access Control Systems

As the name suggests, access control refers to the controls and restrictions placed on access to an organization's premises and assets (physical or virtual). The idea being that an effective access control system exclusively grants access to those who are authorized to enter, while keeping everyone else at bay.

Every organization should clearly define its access control measures and tailor them to the local conditions, in order to ensure accomplishment of its mission. Facility and security managers are focusing on controlling who is allowed entry, when they are allowed, and where they have access.

This control is the foundation of the organization's security program and extends to three equally important areas - credentialing, visitor control and property control:

1. **Credentialing.** This is an administrative process used to validate the qualifications and legitimacy of employees, organizational members, vendors, and contractors by assessing their background.

    - Credentialing devices are used to identify a person having legitimate authority to enter a controlled area. A coded credential (card or key) contains coded information which is machine readable. An electric signal unlocks the door if the prerecorded code matches the code stored in the system when the card is read.

Typical types of cards used include:

A. Magnetic stripe cards which require that the card be swiped through a card reader;

B. Proximity cards which must be passed within several inches of a reader, but not swiped;

C. Smart cards which have a microprocessor and memory, containing personal information embedded into it and must touch the reader in order for the information to be communicated; and

D. Bar codes which are cards, tape, or papers that have coded black bars printed on them. These are read by an optical scanner which is passed over the coded bars and are seldom used for entry control.

2. **Visitor Control**. Most organizations find it beneficial, if not essential, to institute some form of visitor control. From a safety and liability standpoint, control of visitors is important for protecting proprietary information, preventing theft, and as a general good business practice. Visitors should be directed to a receptionist and escorted by an employee inside the organization proper. For obvious reasons, visitors should not be allowed to roam a facility on their own, unescorted. Distinctive visitor control badges, color-coded and dated to be automatically voided at the end of the visit period should be used. Integrated systems are now available wherein occupants can use Web-based wireless technology to communicate and authorize visitor access. A temporary access card can then be issued to the visitor, allowing access to the space. The visitor is then tracked throughout the building.

3. **Property Control**. Property, whether tools used to manufacture a product, office equipment, raw stock, various supplies, or the product itself, must be controlled. Controlling the use and movement of property is difficult without an established process, security measures, and guard force. Strict control over information, inventory, shipping and receiving docks, and stockrooms is necessary. Receiving dock personnel should have locked areas for high theft risk goods and a proper accountability procedure to assure that goods ordered are those received. Shipping docks should be protected by internal fences, locked hold areas, and alert employees who are required to maintain proper accounting procedures.

Strict control over the issuance of organization-owned tools is a necessity. Whenever possible, tools should bear a distinctive organization marking and be signed out to individuals with a bar code tag, or other appropriate identification system. Bar coding is today's technology for recording the tool, its condition, the user, and the date signed out in a database for easy information retrieval and archiving.

Utility Control

Protection of a facility's utility systems should be given high priority. Main transformer distribution areas, fuel storage tanks, and critical HVAC equipment should be protected by eight-foot chain-link security fencing, with minimum clear area of 50 feet. Gas valves and meters, risers, electrical panels, and communications equipment rooms should be locked and protected.

The Goals of an Access Control System

Importantly, an access control system should be robust enough to ensure that even the most tenacious attempts to gain unauthorized entry are thwarted.

Roughly summarized, the primary goals of any access control system are as follows:

- Ensuring those who are authorized to do so gain quick and easy access, without unnecessary delays or complications
- Detecting unauthorized access attempts and providing alerts where unauthorized individuals attempt to gain access
- Stopping forcible or unauthorized attempts to gain access upon detection
- Deterring would-be attackers from attempting to gain access in the first place, due to the difficulties and potential consequences of doing so
- Recording every instance of access (authorized or otherwise) to keep a detailed log of those gaining access and when

Access control systems can be set up in a limitless variety of configurations and with varying levels of security. Nevertheless, the vast majority of access control systems share the primary objectives detailed above.

Identification

In order for an access control system to be viable, it needs to accurately, efficiently and consistently provide positive identifications of those who are permitted to gain access to the area in question. Hence, it must also be able to reliably detect those who are *not* authorized to gain access.

Identification can be provided in any number of forms, though an identification system as part of a security framework will typically use one of three things to assess the individual's eligibility to enter:

- Something that the individual carries, such as an access card or ID tag
- Something that the individual has, as with fingerprints or voice recognition
- Something that the individual knows, such as an access code or password

Access controls and identification systems often combine two or more checks - perhaps the use of an access card and a password. Though in all instances, the organization is fundamentally reliant on advanced technology to ensure only eligible individuals are permitted entrance.

Many of the world's largest and most successful businesses now exclusively use technology-powered entry and exit systems, with no visible manned presence at the doors/gates. The human element is only called for when there is an issue to address, such as an authorized individual who may have misplaced their access card, or someone attempting to gain entry without authorization.

Biometric Access Controls

The field of biometrics has come a long way over recent years, having once existed primarily in the pages of sci-fi novels. Today, even a moderately respectable smartphone may feature the kind of facial recognition and fingerprint scanning technology that would once have been reserved for the highest-security offices and organizations.

The term 'biometrics' refers to the process of automatically identifying or varying the identity of an individual on the basis of their physical traits and behavioral characteristics. Examples of which include fingerprints, iris recognition, voice recognition, signature matching and so on. Many of which have come to be standard components of the access control systems of small and large businesses worldwide

Fingerprints

One of the most accurate ways of identifying individuals by way of their fingerprints. This is precisely why even today, authorities worldwide continue to use fingerprints to identify potential perpetrators in crime scene environments. Each and every fingerprint is 100% unique to the individual in question, making it relatively easy for advanced technology to instantly identify individuals.

Fingerprint scanning and recognition technology is now comprehensively affordable and available in compact devices that are compatible with most modern security systems. The more sophisticated the fingerprint scanning technology, the more difficult it is to gain unauthorized access.

Facial Recognition

Considered by many to be the next evolution in biometric access controls, facial recognition takes things one step further by scanning the individual's entire face. Unfortunately, facial recognition technology remains at a relatively rudimentary stage, with a long list of flaws that need to be ironed out.

Hand Geometry

This is technically a more sophisticated version of fingerprint recognition, which instead of focusing simply on fingerprint patterns scans the hand in its entirety. The geometry of the hand is recorded when the individual is first registered, after which it is scanned and analyzed each time they wish to gain entry.

Though again, issues can occur due to the fact that the geometry of the hand changes continuously as part of the aging process. Even something as simple as weight gain or weight loss can affect the reading provided by a hand geometry access control system.

Biometric Iris Reading

While it's possible for an iris scanning entry system to be extremely secure, there are mixed reports as to the effectiveness of consistency of the technology. It remains a comparatively complex and expensive entry control system, which scans and stores a detailed image of the individual's iris.

As the iris does *not* change dramatically with age, it is considered an accurate form of identification long-term.

Voice Recognition

Speech detection and voice recognition technology is playing an increasingly important role in the way we live our lives. Whether it's controlling appliances via a smart assistant or carrying out web searches hands-free, we now live in an age where we can speak to machines and be understood with reasonable consistency.

Voice recognition is therefore a viable option is part of an access control system, given how each and every person's voice is 100% unique to them. Just as long as a clear reading can be taken of an individual's voice, its' relatively easy for a computer to verify their identity.

However, issues with speech recognition can occur when an individual's voice changes even slightly - perhaps due to having a sore throat or a cold. Intonation when an individual is angry, stressed or in a hurry can also affect voice readings, as can any background noise that may be caring at the time.

In addition, a recording of an authorized individual's voice could be used to gain access to a secure area or system, therefore the technology can be easily deceived.

Limitations of Manual Systems

To a degree, the most effective access control system available to today's business is the system overseen by a skilled human workforce. Even today, relying 100% on technology is impossible in most instances, and inadvisable in all others.

Security is most effective when and the latest technology is combined with experienced and reliable manpower. As for why an exclusively manual system is no longer considered a viable option for most businesses, it's a case of acknowledging the inherent limitations in traditional manual systems.

Examples of which include the following:

1. A forged access card or form of identification may be extremely difficult to identify by manual inspection alone

2. Manually checking the ID of each of and every person entering and exiting the premises can be extremely time consuming

3. Human error can always creep into the equation, such as a lapse in concentration
4. Automated systems can capture and store exponentially more data than a human security officer penning a report
5. Human response times are nowhere near as fast or consistent as those of automated systems
6. The use of technology brings additional accountability into an organisation's security framework
7. It is much easier for an intruder to incapacitate and bypass a human security officer than a high-tech computerised system
8. Human security personnel can be misled, persuaded or bribed - a technology-powered system cannot

Video Surveillance Systems

Second only to a human pair of eyes, a good video surveillance system is the single most important component in a security system. Despite the fact that a video surveillance system doesn't technically *prevent* unauthorized entry or criminal acts of any kind, it can nonetheless be the most effective deterrent at your disposal.

Most criminals are opportunists, which means they take advantage of vulnerabilities and commit crimes where the likelihood of being caught is as low as possible. If your premises are covered by a comprehensive and reliable CCTV system, this sends a powerful and important message to would-be intruders.

Feel free to intrude if you wish to do so, but rest assured you'll be spotted, stopped in your tracks, identified and prosecuted.

Closed circuit television systems (CCTV) provide security personnel with the opportunity to both oversee premises of all shapes and sizes in real time and to refer back to captured and stored footage. Some CCTV systems are fitted with motion detection technology, enabling them to automatically track suspicious or usual activity in any given area.

Of course, a CCTV system is only worth installing if it is capable of doing its job effectively and reliably. Hence, the following considerations should be prioritized when planning the installation of a video surveillance system of any kind:

- The images captured and stored by the video surveillance system should be of sufficient quality to provide accurate identifications
- An additional backup source of power should ideally be available, so as to enable the system to continue operating if the primary power supply fails
- All cameras should be positioned strategically in accordance with nearby sources of light to prevent problematic glare

- Potential ‘blind spots’ should be identified and covered with additional surveillance cameras to prevent intruders taking advantage of them
- The cameras used should be capable of providing clear, complete and high-definition coverage in all visibility and weather conditions
- It should be possible to zoom in on any area of the image at any time, without any loss of quality, clarity or definition
- Once recorded, it should be impossible for the surveillance footage to be edited, deleted or manipulated in any way
- All footage captured and stored should also be time-stamped, providing a clear indication of the time and date it occurred
- Access to stored footage should be heavily restricted, ensuring only authorized personnel are able to gain access to it
- The system should automatically indicate when and where technological issues are encountered with any of the cameras or connections
- Security cameras and related technology to be used outdoors must be 100% weather resistant and approved for outdoor use
- Where possible, a digital backup of all captured and stored footage should be kept, just in case the master copies are lost or damaged

Technological improvements in CCTV now provide for network integration. This means that millions of camera video images can either be hosted on a computer server or, in newer systems, stored internally in the camera. These systems also can access live or recorded video.

Real-time visual camera images can also be sent to Personal Digital Assistants (PDAs), cell phones, and e-mail, any place in the world.

Command centers where camera images are centralized now use intelligent video technology to help with monitoring. It is impossible for individuals to monitor hundreds and even thousands of camera images. Therefore, integration software techniques being used today include camera activation based on specific criteria such as unusual individual behavior, known as behavior recognition, which tracks pedestrians, intruders, and vehicles. This sophisticated software activates cameras when an activity falls outside established parameters. It can be used to create electronic fences that would activate a camera when someone crosses an electronic boundary. Because the fence is electronic, a chain link fence is not needed, thus maintaining the aesthetics of the grounds.

Intrusion Detection Systems

The most effective form of security is that which prevents would-be intruders from attempting to gain unauthorized access in the first place. Where attempts to deter criminals prove insufficient, intruder detection systems form the next line of defense.

An intrusion detection system will not necessarily prevent the individual (or individuals) in question from carrying out their intended criminal acts. However, effective and timely intruder detection can provide security personnel and sometimes local law enforcement with the opportunity to stop them in their tracks.

All intrusion detection systems are designed to be linked with integrated or separate alert systems - audible alarms, flashing lights, sometimes silent alerts sent to police/security personnel and so on. There are various methods by which intrusion can be detected, which in all instances leverage the latest security technology.

Just a few of the most commonly used intruder detection technologies by today's organization include the following:

Magnetic Contacts (Door Switches)

This is one of the most popular intrusion detection technologies for homes and businesses alike. Magnetic contacts are fitted to doors, windows and frames around the premises, which when closed are positioned directly next to each other. The magnetic force of the two magnets then remains stable until the door or window is opened, at which point the magnets are displaced and the alarm is triggered.

Some magnetic contacts are used simply to trigger a 'beep' or 'buzz' when a door is opened, such as in the instance of a fire door or emergency exit. In other instances, magnetic contacts can be used to secure premises out of hours, triggering major security alerts at any point when the magnets are displaced.

Magnetic contact intrusion detection systems are relatively straightforward and inexpensive to install.

Pressure Mats

These are usually used at major entry and exit points, though can be positioned anywhere deemed necessary. As the name suggests, the technology involves the positioning of a pressure-sensitive piece of material, which when stepped on (or driven over) triggers an alert accordingly.

Pressure mats must be designed in a way so as to prevent false alarms in the event that small animals or general debris was to come into contact with the mat. Some organizations prefer to keep pressure mats invisible, while others deliberately draw attention to them to create a visible deterrent.

Vibration Detector

Vibration detection technology is most commonly used as an additional safeguard for security fencing. As many types of fencing are technically quite easy to cut through and penetrate, additional measures must be taken to deter and prevent potential attacks.

When a vibration detector is installed, it automatically detects suspicious vibrations in the materials of the fence and triggers an alert accordingly. Vibration detection systems can be tailored to simply illuminate the area in question when unusual activity is detected, or send an alert directly to security/police personnel.

Glass Break Detector

Glass break detection technology has been around for some time that has become increasingly sophisticated over recent years. Simple to install and generally reliable, the system is designed to provide an alert and/or sound an alarm in the event that the glass in question is broken.

An effective glass break detection system may also be configured to note unusual vibrations. In which case, the window, door or protective glass screen in question does not necessarily have to be broken for the alarm to be raised. Security personnel are alerted when the unusual activity is initially detected, allowing for them to take earlier action.

Active Infra-Red Barrier

More commonly used in advanced high-security settings, an active infra-red barrier can use a single beam or multiple beans to detect activity in complete darkness. When the beam is disturbed or broken, it generates an automatic alert or triggers an alarm accordingly.

However, active infra-red barrier to acknowledge technology has a tendency to prompt false alarms, as it can be affected by adverse weather conditions, surrounding vegetation and even pieces of debris carried on the wind.

Laser Detection System

Many installations continue to use laser detection systems for the protection of high value assets. Such systems are designed to cover high-security areas with a complex configuration of invisible laser beams, which when broken automatically trigger an alarm.

An effective laser detection system can be comparatively complex and costly to install, though can also be an extremely reliable and practically impenetrable safeguard. Though the importance of ensuring a backup source of power is available cannot be overstated, as a laser security system will offer no protection at all if the power is cut off.

Further Reading:

- ✓ Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies Kindle Edition by Jonathan B. Tucker (Editor), 2016
- ✓ MDM: Fundamentals, Security, and the Modern Desktop: Using Intune, Autopilot, and Azure to Manage, Deploy, and Secure Windows 10 1st Edition by Jeremy Moskowitz,