UNIT-15

Facility Security Management

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

Unit 12

Facility Security Management

Physical security has always been a major consideration for most organizations. It has taken on more importance in the last ten years because of terrorist incidents like the attacks on civilian targets in Europe, the Middle East, Asia, and the shootings at various business establishments, universities, and schools. In addition, theft of information is on the upswing. The continuous thefts of laptops and hard drive computer information have resulted in compromising the private information of thousands of individuals.

Today's global business environment requires organizations, including higher education, to take security seriously by developing a security plan. This means that facility managers have greater responsibility and are being asked for their recommendations concerning security.

Every facility manager must think about physical security and assist with developing a security plan in conjunction with their security counterparts. The result of a facilities security plan is the protection of employees, assets, and products of an organization from threats, without and within.

Facility Physical 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, with carefully defined policies and 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 managers are concerned with the general organization goals, they also have immediate specific goals which are discussed below.

Protect People and Property

- building codes and safety requirements include special security precautions
- hardening buildings against structural damage,
- building wider stairwells for evacuation,
- pressurizing stairwells to eliminate smoke,
- improving fireproofing,
- building air intakes which are inaccessible from street level,

- detailing building evacuation plans,
- reinforcing elevator shafts so that they could be used forevacuation,
- providing backup emergency lighting,
- using photoluminescent paint and electroluminescent light strips in stairwells, and

Facilities Security Responsibilities

Facility managers and security managers share responsibilities for protecting an organization's people and assets. It remains unclear which manager has the overall responsibility (it varies from organization to organization and often depends on individual personalities). The distinction is hazy when compounded with new electronic technologies and leads to the question: who should lead the physical security effort for an organization or a facility?

The future of physical security involves the information technology manager, security manager, and the facility manager. There will have to be collaboration and cooperation between all three if the organization's physical security program is to work efficiently and effectively. The intertwined nature of operating facility systems such as access control, life safety systems, heating, ventilation and air-conditioning (HVAC), lighting, and environmental monitoring illustrates the importance of communication and collaboration when planning facility renovations. Emergency pre paredness, damage assessment, structural integrity of facilities, and evacuation plans are areas in which facility managers must have greater knowledge of functional needs because of the daily involvement and interaction. The responsibilities of facil-ity managers, security managers, and the information technology manager are shown in Fig: 9.1, 9.2, and 9.3. Additionally, employees play an important role in safeguarding and securing the organization's assets, especially those assets that are sensitive and critical. Whether understood or not, the responsibilities of employees must be considered.

Fig: 9.1. Facility Manager Responsibilities

- Create a facility management program which helps reduce security risks
- Develop an understanding of current physical security trends
- Assist with developing cost effective security solutions to meet upcoming facility and organization requirements
- Ensure proper planning, evaluation, application, design, installation, and construction of facility enhancements for all aspects of physical security
- Provide criteria and guidance to ensure the proper design, installation, and acceptance testing of all organization projects related to physical security
- Identify problem areas that impact security design
- Coordinate physical security surveys with public safety offices
- Coordinate with the security manager during the planning, design, and construction phases of all construction projects to identify physical security requirements
- Provide equipment and manpower to support security measures

- Ensure that backup power systems will function when needed
- Obtain computer training on integrated systems beyond the basic skills

Fig: 9.2. Security/Safety Manager Responsibilities

The organization public safety officer will:

- Recommend physical security considerations according to the organization's mission and vulnerability to terrorist acts, criminal acts, or other disruptive influences
- Conduct physical security surveys and inspections in conjunction with the facility manager
- Coordinate with local law enforcement offices
- Monitor the resource management of the organization's physical securityprogram
- Coordinate the organization's physical security requirements with the facility manager including immediate requirements as well as planning, design, and construction projects
- Review all planning documents and construction plans and specifications for construction and renovation projects at all stages ofdevelopment
- Establish and enforce uniform security standards and procedures
- Have a thorough understanding of the organization's businessplan

Fig: 9.3. Information Technology Manager Responsibilities

- Integrate information security procedures into all business processes
- Create and implement a Computer Emergency Response Team (CERT)
- Determine existing information security capabilities (e.g. firewalls, password protection, and network security)
- Establish the need and verify the functionality of emergency power back-up systems
- Determine and verify offsite data storage
- Conduct an information technology gap analysis to determine shortcomings and what measures should be implemented to mitigate exposur
- Develop information security plans to contain a security breach and the restoration of critical data
- Plan and conduct mock information securityexercises

All employees must understand that security is a responsibility not to be taken lightly. Employers can influence how their employees respond by taking some simple steps.

1. Educate employees on their roles and responsibilities, the link between security and preparedness, and the cost of providing security which ultimately impacts them.
2. Invite employee participation and suggestions in developing security plans. People who participate in planning are more likely to cooperate. One suggestion is to ask them to develop scenarios for how they would attack, penetrate, or compromise their facility.

3. Cultivate and continue nurturing employee awareness of security. Employers can do this through the use of newsletters, sending information through the organization intranet, staff meetings, and other communications tools.
4. Empower employees by providing them with knowledge of the security plan and the resources they have available. This will diminish their fear and anxiety and encourage their contribution to the security of the organization.
5. Promote personal and family security as part of the organization's security plan. This will encourage employees to be observant and report unusual activity.
6. Integrate information concerning the security plan with other organization initiatives such as employee safety and accident reporting. This will soften the emphasis on security and allay fears and anxiety by making safety in the workplace the primary concern.
7. Conduct security drills and exercises. Including employees provides them with a sense that they are contributing to the organization's security plan, building their confidence, and developing the perception they are part of the plan.

Security Planning Considerations

Facility managers are responsible for operating and maintaining every aspect of a facility. As a result, they must be involved in the security planning from the outset. They know the day-to-day quirks and workings in a facility better than anyone else and can provide insight and verification of what security measures should be taken.

Review of Security

Every organization should review its overall physical security needs with regard to the facility location, layout, design, and construction. This includes assessing the effectiveness of external and internal controls, and how they pertain to deterrents, control points, authorization levels, hardware, and security devices. Effective security plans include the need for personnel screening prior to employment, and for continued evaluation, monitoring, and assessment. This is extremely important, especially, in high risk areas.

Control and enforcement of a facility must be exercised concerning authorization levels, key usage, access restrictions, sign-in, and sign-out procedures, opening and closing procedures, and surveillance. All security violations must be documented. Written policies must be developed defining classifications and restrictions on handling this sensitive information. Finally, an education and training program should be established emphasizing the need for continuous security.

Planning Process

All of the above is important when it comes to security, but how does the facility manager make it all happen effectively? It starts with planning, and the facility manager and chief security officer are the catalysts responsible for developing the blue-print of a security plan. They initiate the planning process

which includes: organizing and leading the security planning team, developing the security plan, implementing the plan, and measuring the results. Since no two organizations are exactly alike, each security plan must be developed to fit each situation.

The plan serves three important functions. First, it clarifies, focuses, and matches security requirements to the organization's mission. Second, it provides a logical and systematic methodology for implementing those requirements. Finally, it provides a point of reference against which achievement of established goals can be measured and analyzed.

Planning Team

At a minimum, the planning team must include the following: facility manager, chief security officer, information technology manager, safety manager, and any stake-holder who would be impacted by or required to support the plan. Clear guidelines must be established with the initiation of the team and include such considerations as meeting times and duration, agendas, individual responsibilities, timelines, plan expectations, and the final deliverable.

Security Planning Approach

When developing a security plan, the planning team must focus on four areas: assessing the organization's security need (the risk); addressing those needs through the security plan; implementing the plan; and continuous review, adjustment, and testing of the plan. The final plan must be realistic, supportable, and affordable.

1. Assessment. Judge the current state of security within the organization. This could be done using internal organization resources or by outsourcing to a security consultant. The assessment should match the current state of security against the desired state. A good technique to use is to conduct a strengths, weaknesses, opportunities, and threat (SWOT) analysis. Determine the current strengths of organization security, the current weaknesses, opportunities to improve the current state of security, and identification of threats that need to be considered. Another term for this would be vulnerability assessment.

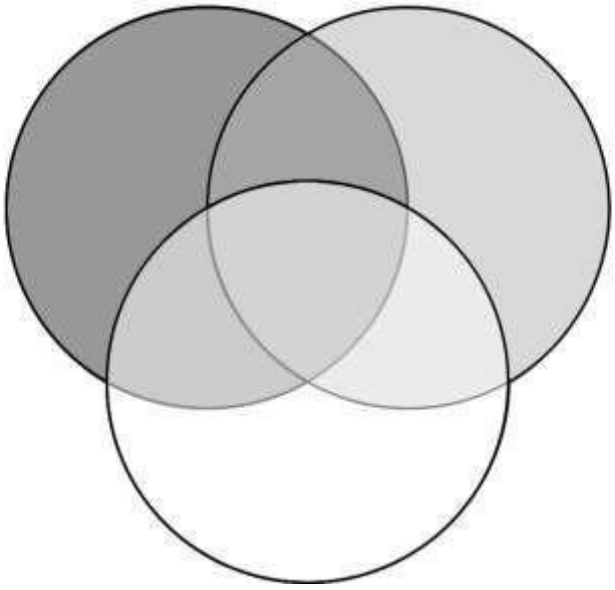
2. Developing the Plan. The planning team will have to answer questions concerning the what, when, where, and how of planning for security. Some of these answers will have to come from interviews with senior organization executives.
   - **What:** What are the goals and vision of the organization over the next five to ten years? What changes does the organization see coming that will impact security? What security issues and risks exist currently? What assets have to be protected? What will be the short and long term costs of the security requirements?
   - **When:** What period of time is being considered? What is the timeline if the organization is planning to grow in size?

- **Where:** Will the organization remain in the same geographic location, or expand into new markets? Is it planning to purchase or lease new space?
- **How:** How will security support the current mission and future vision? How will the sense of ownership of the plan be inculcated in all employees? How will progress be measured?

3. Plan Implementation. Implementation of the plan is driven by answers to the above questions and its associated costs. Consider organizing the procedures into smaller prioritized action plans which will make them more palatable and achievable. Finally, develop training for the staff, implement technology that matches the risk, and initiate policies and procedures to administer the plan.
4. Components of the Plan. Security plans can be divided into three components: physical security, operational security, and technological security. See **Fig: 9.1.**
5. Priority. Depending on what is involved and the cost to implement, the plan may be phased in over time. Trying to implement a complete plan at one time may be overwhelming and too costly for the organization. Some parts may be simple and easy to implement the first year. The more

Fig: 9.1. Components of Security

- Sceurity
- Physical security
- Technological security
- Operational security



The physical security component is focused on the obstacles and barriers. This is the application of barricades, fencing, gates, 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.

- **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 currentconditions.
- **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.

Communications

Communication with employees, security and facilities staff, and occupants and visitors is the most important action that can be taken. Everyone wants to know what is happening and unless they are told, their anxiety will increase. Listed below are a variety of simple methods to achieve this.

1. Scheduled Training. All new occupants and new employees must be scheduled to attend emergency/security training within the first two weeks of employment.

2. Newsletters. Distribute periodic newsletters to inform people of any revisions to the security plan and to update them on technology.
3. Available Technology. Text messaging is now common and being used by many organizations. This technology allows for hundreds, or even thousands, of people to be notified within minutes of the need to shelter-in. Another simple but effective tool for mass notification is the use of a siren, horn or whistle. When an organization uses this method of mass notification, people recognize the alert and prepare to shelter-in.
4. Conduct Periodic Drills and Exercises. Develop realistic scenarios that the organization could face, based on the threat assessment and associated risks. Plan periodic drills and occasional exercises for all organization employees.
5. Public Address Systems. Public address systems provide a means of notifying many individuals of dangerous situations and giving them instructions as to what they should do.
6. Alarms. Duress alarms are important in specific situations. Individuals in key and sensitive positions, such as bank managers, school principals, business executives, teachers, etc. can be threatened and accosted. Duress alarms provide them with the ability to silently notify authorities that an emergency situation is occurring.

Crime Prevention Through Environmental Design (CPTED)

There is more to security than locks, keys, alarms, and cameras. When planning to renovate or construct a new facility, security should be a major consideration. Crime prevention through environmental design (CPTED) was originally conceived in the late 1960s. The theory of CPTED is based on the concept that design, using information from the built environment, can have a positive impact on reducing crime and improving quality of life. According to CPTED security consultants, a private consulting firm specializing in security, there are four built environment strategies which should be used in design guidelines when preparing a facility security assessment.

Natural Surveillance

In theory, if someone knows they are under surveillance, that person is less likely to commit a crime. Integrating this definition with design guidelines to maximize visibility would tend to dissuade criminal activity. Examples would include the following:

- Have windows overlooking open areas such as parking lots, sidewalks, and entrygates.
- Keep window shades and blinds open.
- Landscape areas near buildings and other key locations in such a way that monitoring and surveillance are maximized.
- Use outside lighting to reduce shadows and blind spots

Natural Access Control

The intent of access control is to channel personnel and vehicles to specific locations where access is controlled. Examples include:

- Having one main entrance to a building or parking facility where everyone who enters can be checked.
- Elevating vegetation located near buildings at least six feet to eliminate locations where someone can hide.
- Ensuring storefront entries are kept clear, allowing easy visibility for security officers.
- Closing off access to stairwells and ladders to prevent perpetrators from gaining entrance to roof tops.
- Using fencing, locked gates, and masonry walls to direct people toward specific entrances.

Territorial Reinforcement

Territorial reinforcement makes use of design features to discourage criminal activity by making the intruder stand out. This is done by defining the property boundaries using fencing and gates, landscaping, signage, and sidewalk and roadway pavement. The intent is for security officers and employees to more easily identify individuals who do not belong. This strategy tends to make authorized personnel feel more protected whereas unauthorized individuals feel uncomfortable.

Maintenance

Maintenance of a facility provides a glimpse into how well a facility is managed. It can give a positive impression, or a negative one. Deterioration of surroundings is seen as a weakness and, therefore, criminal activity is more apt to occur. Examples of conditions that convey a perception of weak security and encourage crime include the following:

- Insufficient lighting resulting from broken and un-repaired lights.
- Inoperable emergency call boxes.
- Fencing in a state of disrepair, or with gaps and holes in the fencefabric.
- The broken window theory underscores the need for maintenance. Broken windows, if left unattended for a long period of time, generate a perception that the organization is deficient and could devaluate property into a blight condition.

Vulnerability Assessment

Understanding the potential vulnerabilities of a building design helps with making decisions concerning structural integrity, building envelope, architectural design, facility perimeter security, and safety requirements. Today, vulnerability simulations and modeling allow building owners, facility managers,

and security managers the opportunity to visualize where potential problems may occur and the impacts those problems will have on the facility, occupants, and the mission of the organization. This capability enables decision makers to better understand the issues associated with various security scenarios, how they impact new construction and renovations, and how they can mitigate risks faster and more effectively.

1. **What is a Vulnerability Assessment?** Once known, potential threats to an organization can be mitigated by taking specific corrective actions to reduce or eliminate the threat. These vulnerability assessments are used in developing and prioritizing security plans, modifying existing operational procedures, and making policy changes where necessary to protect critical assets.
2. **Why Assess?** Organizations need to understand the impact of the threat they could face. Vulnerability assessments provide the understanding of the risks and threats. This information can then be used to develop options to combat the risks and threats. Periodic reviews and updates of the assessment should be conducted to identify changes in threats and risks and how these changes impact the security plan.
3. **Who Assesses?** The conduct of a thorough vulnerability assessment involves an understanding of people, culture, science, and engineering. Therefore, several individuals having expertise in each of these areas should be consulted.
4. **Techniques Used?** The vulnerability assessment process varies in complexity based on the organization's mission. The process is founded on various factors which include: size, population impacted, evaluation of existing countermeasures, analysis of current risk, state of infrastructure, knowledge of and types of potential threats, available security technology, applicable local, state, and federal regulations, and other factors germane to the organization. Elements of a vulnerability assessment are depicted in **Fig: 9.2** and describedbelow.

A. Provide a description of organization mission and goals. Consider the following:

   1. Priority of services provided?
   2. Who are the customers?
   3. What are the assets and processes most important to achieve the organization mission and goals?
   4. What are the organization's contractual obligations?

B. Identify and prioritize detrimental situations and conditions to avoid. Consider the following consequences:

   1. Economic impact to the organization
   2. The lack of employee confidence in the organization's ability to provideprotection.
   3. Problems arising from specific events.

C. Identify critical organization assets which would be impacted by some type of attack or intruder. Consider the following:

1. What could an attacker do to disrupt the operation of critical facilities, assets, or processes?
2. Has a vulnerability assessment been conducted concerning the operation and maintenance of physical barriers, facility infrastructure, and electronic, computer, or other automated systems?

D. Conduct a probability assessment of the potential that such an attack or criminal action could occur. Consider the following:

1. What modes of attack would impact critical assets?
2. Is there a specific scenario that is more likely?

E. Evaluate existing countermeasures. Consider thefollowing:

1. What physical security capabilities are currently used for detection, delay, and response?
2. What cyber security capabilities (firewalls, security protocols, wireless data, and voice) are currently used?
3. What security policies (personnel security, physical security, lock and key control, credentialing, security drill and exercise records) and proceduresexist?

F. Review and analyze risks, and make recommendations to reduce those risks. Consider the following:

1. What are the current risks?
2. Will recommended risk reduction actions reduce vulnerability?
3. What strategies should be considered to reducevulnerability?
    a. Examine current business practices. Do current policies, procedures, and training support the need for improved security?
    b. Examine system upgrades. Will changes in operations, equipment processes, or infrastructure make the organization safer?
    c. Examine security upgrades. Will improved detection and response capabilities make the organization safer?

New Facility

The importance of prior planning for security in a new facility cannot be over-stressed. Incorporating the amount of security desired at the time of preliminary architectural planning will result in cost savings and will provide senior management an early look at the overall security plan and its cost. Management will then have an opportunity to make positive security-oriented decisions that

otherwise might be brushed aside if they have to be added as an afterthought. Planning should not be totally confined to the facility under construction but should be done with an eye to expansion possibilities five and ten years in the future.

Personnel entrances, parking facilities, and guard control points should be carefully planned as well. The security of docks and a central location for shipping and receiving should be considered. Vehicular and pedestrian traffic should not be routed through areas of this nature.

Utility security should be designed into the overall site plan. This includes electrical switchgears, HVAC equipment, emergency power generation equipment, emergency water sources, standby fuel supplies, and transformer banks. It is at this time that fencing and outside lighting, entrance gates, lobby security, guard posts, alarm systems, vaults, docks, warehousing requirements, and internal security requirements are considered. The utilization of industrial hardware and lock and key requirements are discussed, reviewed, and implemented at this time as well.

Leased Facility

Prior to leasing or purchasing an existing building or facility, a physical security survey should be conducted to assess security needs commensurate with facility use. All door locks should be changed prior to occupying the facility. This could be a problem if inferior hardware has been used in the original construction; however, the expense of converting to a heavy duty system is worth the cost. Consideration must also be given to crash-out doors, windows, roof hatches, outside ladders, utilities, skylights, ventilators, manholes, subterranean ducts, storm drains, lighting, fencing, and parking garages. The security of most of these items should be covered in the lease agreement.

Construction Site

Construction, when it directly involves security, should be carefully planned and monitored. Security of sensitive rooms such as telephone closets, control lighting booths, and mechanical spaces must not be overlooked. Tool cribs and similar storage areas should be constructed using solid walls and a roof covering whenever possible. Facilities housing organizations handling large sums of money, such as banks and credit unions, should have adequate safes and well planned work areas fitted with alarm systems, including duress alarms, when applicable.

Facility security Implementation

Technology Today

Prior to the Internet revolution, security systems were operated via cable and telephone lines. Surveillance was limited to local coaxial cable and by today's standards, considered relatively slow. The internet has enabled systems to operate at the speed of light from anywhere in the world and with wireless capability. Remote monitoring is commonplace. Security systems such as closed circuit

television images (CCTV) and access control functions can be monitored from handheld personal digital devices.

There is disagreement concerning which tools, systems, or technologies are best for running security programs. Some facility managers are opting for security audits to help resolve this uncertainty. Additionally, technology has far surpassed the evolution of trade association-approved-and-accepted written security standards and guidelines.This has greatly complicated the issue and resulted in individual standards being developed.

The issue for facility managers is to balance security requirements against facility operational needs and budgetary concerns. All three conditions are achievable by integrating current security technology with core building services systems. The synergy gained by this integration will help provide better security, make more efficient use of facility operational systems by improving the diagnoses of everyday situations, and ultimately reduce cost through efficiency and conservation. Using integrated systems, facility managers can secure a facility and at the same time detect heat loads, adjust the heating and cooling accordingly, synchronize elevator usage to peak employee arrival and departure times, adjust vendor delivery times to minimize impacts which can cause parking congestion, and adjust maintenance support schedules such as cleaning. The same can be done with lighting. Not only is the facility physically secure, its core building systems are adjusted to meet the need. This helps to fine tune the operation of the facility and maximize building automation systems to support occupants while concurrently decreasing operating expenses.

Integration of facilities, safety, and security systems is advantageous and timely. With careful planning, integration of systems can result in greatly enhanced security and safety. For example, pedestrian door control can be integrated with the CCTV surveillance system, the elevator system, the fire protection system, automatic door opening hardware, emergency call boxes, parking gate arms, etc.

Access Control

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.

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 printedon 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.

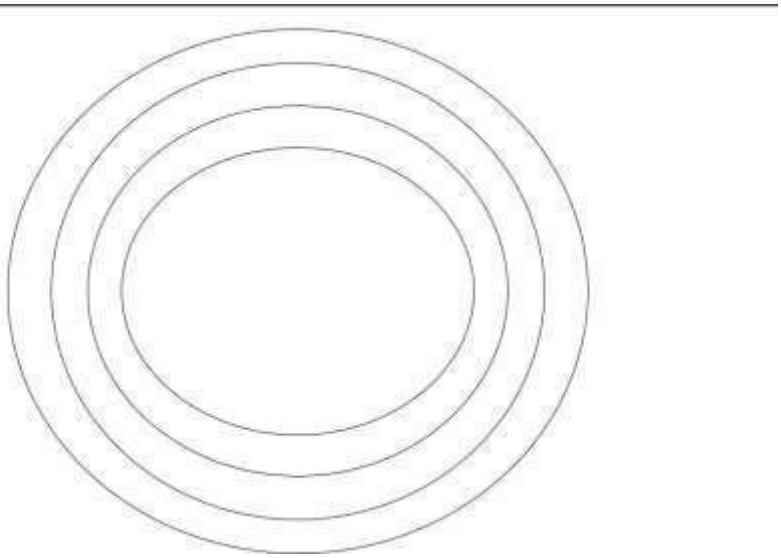
Physical Deterrents

Physically barring access to the facility is the first line of defense. Physical security provides a deterrent to intruders and it forces those interested in committing a security violation to think twice. A good physical security plan incorporates a multi-level security system, also called a layered approach

1. **Outer Layer.** This layer consists primarily of barriers and deterrents such as fences, bollards, angled steel plates called wedge barriers that can be hydraulically raised, anti-ram gates, lighting, signage, security guards, intrusion alarms, mechanical locks, biometric locks, and credentialing. The purpose of this layer is to discourage trespassing.
2. **Middle Layer.** This layer includes such areas as: doors and glazed and film coated windows, ventilation ductwork, roofs, and ceilings. The purpose of this layer is to provide prevention of access and early warning of facility penetrations.

- Core
- Outer layer
- Middle layer
- Inner layer

Fig: 9.2. Security Layers



3. **Inner Layer.** The inner layer controls movement and secures interior space within the facility by reinforcing door and window access control, security guards, signage identifying unauthorized areas, lock systems, closed circuit television (CCTV), safes, and vaults.

Ideally, the security plan will integrate natural, man-made and human deterrents and enable the organization to achieve a layering of security as previously mentioned. This integration will keep the security plan flexible and easily adaptable to the current situation. Examine the security of your facility from an intruder's viewpoint.

A. **Natural Deterrents.** Natural protective deterrents are ditches, water obstacles, or other terrain features that are difficult to traverse. Good security planning makes use of these features to help dissuade unwanted intrusion.

B. **Man Made Deterrents.** Security of a facility requires that access into it be controlled. This can be achieved by the use of structural barriers and other forms ofdeterrence.

1. **Structural Barriers.** Structural protective barriers are man-made devices such as fences, bollards, walls, floors, roofs, grills, bars, road-blocks, or other construction that are used to restrict, channel, or impede access. Protective barriers form the perimeter of controlled, limited, and exclusion areas. Utility areas such as water sources, transformer banks, commercial power and fuel connections, heating and power plants, and air-conditioning units may require these barriers for safety. Barriers create a psychological deterrent for anyone thinking of unauthorized entry. They may delay or even prevent passage. This is especially true of barriers against vehicles and forced entry.
2. **Turnstiles.** Turnstiles have been used for many years as a means of controlling entry into a facility. They are simple and often overlooked or not considered for access control. Today, with improved technology, turnstiles can be either mechanical, optical, orvideo.

a) Mechanical turnstiles control entry by restricting the direction in which someone can transit the entry point. They can be designed to operate with card readers, coins or tokens, electronic keypads, etc. The advantage of these functions is that they do away with guard control. A suitable barrier must be installed above the top of the turnstile to prevent persons from using it as a step ladder for access over afence.

b) Optical turnstiles channel pedestrian traffic into lanes where infrared beams create an invisible electronic field. As pedestrians move through the field they are monitored and information is stored in micro-processors. These electronic fields have the ability to distin-guish human beings from objects. This security monitoring equip-ment is best suited for high volume pedestrian locations such as buildinglobbies.

c) Video turnstiles are used extensively in Europe. These are primarily tools used for counting the number of people entering and departing a specific location such as a store or shop, bank, library, restaurant, etc. These turnstiles function by having a closed circuit television camera, which is connected to a computer, located at the entrance to the facility. When someone crosses its path, a count is logged into the computer. Video turnstiles are used when there is a large volume of people and it is important to determine the number of people entering and leaving an establishment.

3. Lighting. Security lighting should be used as a psychological deterrent and should also be used along perimeter fences when the situation dictates that the fence be under continuous or periodic observation. Lighting is relatively inexpensive to maintain and reduces the advantages of concealment and surprise for a determinedintruder.

a) Security lighting is desirable for those sensitive areas or facilities with-in the perimeter that are under observation. Such areas or facilities include loading dock areas, vital buildings,

storage areas, parking areas, and vulnerable control points in communication and power- and water-distribution systems. Security lighting has considerable value as a deterrent to thieves and vandals and may make the job of the saboteur more difficult. It is an essential element of an integrated physical-security program.

b) A secure auxiliary power source and power-distribution system at the facility should be installed to provide redundancy to critical security lighting and other security equipment.

c) When planning for security lighting, the facility manager should consider the following.

- Cost of replacing lamps and cleaning fixtures, as well as the cost of providing the required equipment (such as ladders and lifts) to perform thismaintenance
- Provision of manual-override capability during a blackout, including photoelectric controls
- Effects of local weather conditions on lighting systems
- Fluctuating or erratic voltages in the primary power source
- Grounding requirements
- Provisions for rapid lamp replacement
- Use of lighting to support a CCTV system

d) Re-strike time (the time required before the light will function properly after a brief power interruption)

Illumination and color. Metal halide, white light, is now the preferred light for security.CCTV-Camera lighting requirements. The following considerations apply when lighting systems are intended to support CCTV assess-ment or surveillance.

- Camera's field of view
- Lighting intensity levels
- Maximum light-to-dark ratio
- Scene reflectance
- Daylight-to-darkness transitions
- Camera mounting systems relative to lighting
- Camera's spectral response
- Cold-start time
- Re-strike time

Facility Electronic Security

1. **Duress Alarms.** Duress alarms are used to signal a life-threatening emergency. They often are identified by terms such as: panic alarm system, personal alarm system, man down system, emergency nurse call system, and employee security system. These alarm systems have a myriad of applications but are most commonly used as senior citizen personal alarms, correction facility officer personal alarms,epilepsy alarms, environmental hazardous emergency

alarms, and personal security alarms. They can be fixed or portable and are usually manually operated.

A. Fixed duress devices are mechanical switches mounted at inconspicuous locations such as under a desk top or on the floor. They can be easily activated by a push button, or foot operated if located on the floor.
B. Portable duress devices are wireless and consist of a transmitter and receiver. The transmitter is usually small enough that it can be worn or carried. The receiver is positioned in a fixed location within the facility and transmits a signal or is hardwired to an alarm monitoring station.

2. **Electronic Entry Alarms.**

A. **Electronic detection systems**. These should be capable of detecting individuals crossing a detection zone by walking, crawling, jumping, running, rolling, or climbing a fence. Current technology includes active infrared, microwave, buried line (e.g. fiber optic and coaxial cable), fence-mounted sensors, video motion detection, linear beam (e.g. electronic fence), and glass-break sensors (e.g. acoustic and shock).
B. **Door and hatch contact alarm switches**. Electric strike locks should be used for interior doors. Magnetic door contact switches should be installed at all building exterior doors to monitor doors which are propped or forced open. Care must be exercised in designing for the use of these locks on doors used for egress to ensure egress is permitted at all times, especially with fire alarm activations. Exterior facility locations such as entry hatches or equipment vaults should be equipped with high security magnetic switches. Industrial doors and roll-up doors should have high security wide gap magnetic switches.

3. Biometrics. Biometric devices are used to control entry based on the measurement of one or more physical or personal characteristics of an individual. They consist of a reader and scanning device, software which converts the collected information into digital form, and a storage database for future retrieval. This technology is spreading and is currently used for time and attendance reporting, facility access, and signature verification. Some organizations are now combining biometrics with smart card usage to raise the level of security and minimize breaches.

Various types of usage of biometrics are depicted below.

A. **Fingerprint Scan**. An individual's fingerprint is scanned and matched against what is stored in the organization's database. It is used for positive verification of the individual for access to a space, verification of time and attendance, permission of

access to equipment and sensitive records, desktop usage, and transportation. Its use is limited only by our capacity to find ways to use it.

B. **Iris Recognition.** This is the most accurate of all biometric technologies. It's used primarily in high security locations such as government and private research centers, correctional facilities, and financialinstitutions.

C. **Hand Geometry.** This technology is used in high security facilities where there is an expectation of a harsh environment such as extremely cold or hot temperatures. Examples include nuclear facilities, construction sites, or maximum security correctional facilities.

D. **Facial Recognition**. This biometric technology is continuing to evolve. It is not used extensively today, but that will change with time and improvements. Currently, three dimensional technology (3D) is being developed, it will be integrated with improved lighting capacity, and will have the ability to rotate an image. This technology appears to be the future of biometrics as far as application and acceptance. It is discreet and passive.

E. Other Biometric Technology.There are many variations of biometric technology, including voice biometrics, signature biometrics, and DNAbiometrics.

4. **Closed Circuit Television (CCTV).**

A. 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.

B. These digital systems now enable quick and easy locating of images in the database based on the time of the incident. Other capabilities include the triggering of cameras based on motion detection or alarm activations. Some jurisdictions, for example large cities such as Los Angeles or Las Vegas, are now requiring visual confirmation of an activated alarm prior to responding.

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

D. 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.

Employee Protective Measures

1. **Insider Threat.**

Security intrusions or thefts by employees amount to several billion dollars annually. Many companies prefer to believe such security breaches or thefts are really not happening or would not happen to them. Often, employers will not take action against offenders, and they are even reluctant to impose additional security measures to lessen losses. Measures that will improve security and lessen theft should always be considered. Fig: 9.3 lists the actions that employers should take.

Employer Protective Actions

- Conduct careful pre-employment screening.
- Consider implementing a company sales program for surplus equipment. Ensure computer equipment is wiped clean of data before being sold or given to charitable organizations.
- Apply well-publicized disciplinary action for those caught stealing.
- Control employee and visitor pedestrian traffic through entrances.
- Maintain tight inventory control.
- Utilize an organization property pass system for removal of all organization property from the premises.
- Install signage at all entrances stating that packages, and vehicles entering the area inside the organization's perimeter, are subject to periodic searches.
- Shipping and receiving areas should be off limits to unauthorized employees.
- Emergency Phones.(also known as emergency call boxes) can be installed any-where because of technology today. Wireless cellular capabilities enable these emergency communications systems to be located in remote locations such as elevators, parking garages, parking lots, sidewalks, and along isolated roads. These phones must be clearly identifiable from a distance because they are to be used for true emergencies. They should be easily activated by simply pressing a button or removing the receiver from its cradle.

Further Reading: