Certified Protection Officer Program

Chapter 14

Physical Security Concepts and Applications

Learning Objectives

Students will be able to:

- Define physical security planning.
- List the five steps in the security planning process.
- List the three options for intrusion monitoring.
- Explain the three objectives of security lighting.
- Name different types of locking hardware
- Provide the three roles of CCTV and access control.
- Identify the correct height for security fencing
- Explain the fire safe temperature for paper
- Explain what convergence is
- Conduct a facility tour to explain to the class the physical security measures present.

Purpose

Physical security is a vital part of all security planning and is fundamental to the protection of people, property and assets. Without physical security protection would be difficult or even impossible.

Key Terms

- Physical Security Planning
- Occurrence Probability Factors
- Quantitative Categories
- Threat Level Matrix
- Layered Security
- Glazing
- Convergence

Engagement

https://www.youtube.com/watch?v=GxAknTEfC2M

Why is monitoring and intrusion technology more effect than patrolling?

Do you feel it is cost effective?

What is physical security planning

- Security process that, if followed, will result in the selection of physical countermeasures based on appropriateness. Countermeasures should also be justifiable from a cost point of view.

- The organization identifies its:
    - Assets,
    - Risks,
    - Threats

    which then determine the level of appropriate countermeasures that are required based on this process.

Risks

Categorized into three areas:

1. ***People***
2. ***Property***
3. ***Legal Liability***

Security planning process consist of 5 steps

1. Assets are identified.
   - *People are most important then everything else*
2. Loss events are exposed.
   - Industrial disasters
   - Natural disasters
   - Civil disturbance
   - Crime
   - Other threats
3. Occurrence probability factors are assigned.
4. Impact of occurrence is assessed.
5. Countermeasures are selected.

Occurrence probability factors are assigned

The following can affect probability:

- The <u>physical composition of structures</u>:
    - wood frame
    - concrete block

- The <u>climatic history of the area</u>, such as:
    - frequency of tornados
    - hurricanes
    - earthquakes

Occurrence probability factors are assigned

- The <u>nature of activity at the property to be protected</u>:
  - if the products being produced are televisions
  - related products
  - probability for theft will likely be high
- The <u>criminal history</u> for the local and adjacent areas
- Is there <u>community conflict</u> in the area

The probability or an occurrence

1. Certain
2. Highly probable
3. Moderately probable
4. Improbable

Quantitative categories: To make these words more meaningful, we can assign percentage weights to each:

- Certain 75 – 100%;
- Highly probable 50 – 75%;
- Moderately probable 25 – 50%;
- Improbable 0 – 25%.

Impact of the occurrence

1. Very serious
2. Serious
3. Moderately serious
4. Unimportant

These categories should be assigned a financial value.

Countermeasure selection
Threat Level Matrix

Threat Level Matrix

	Improbable	Moderately probable	Highly probable	Certain
Unimportant	I	I	I	I
Moderately Serious	I	II	II	II
Serious	II	III	III	IV
Very Serious	III	IV	IV	IV

Levels of Security
I   Low
II   Medium
III High
IV Very High

FIGURE 14-1   Threat level matrix.

Security-in-depth

- Also known as layered security:

  - *A process of placing progressively more more difficult obstacles in the path of the aggressor.*

- First line of defense:

  - **generally the property line. Can be natural(river), man-made (fence), physical or psychological.**

Security-in-depth

- Second line of defense:
  - *exterior of the building. Remember the building has six sides. Special attention to be given to points of entry.*
- Third line of defense:
  - *interior controls or object protection.*
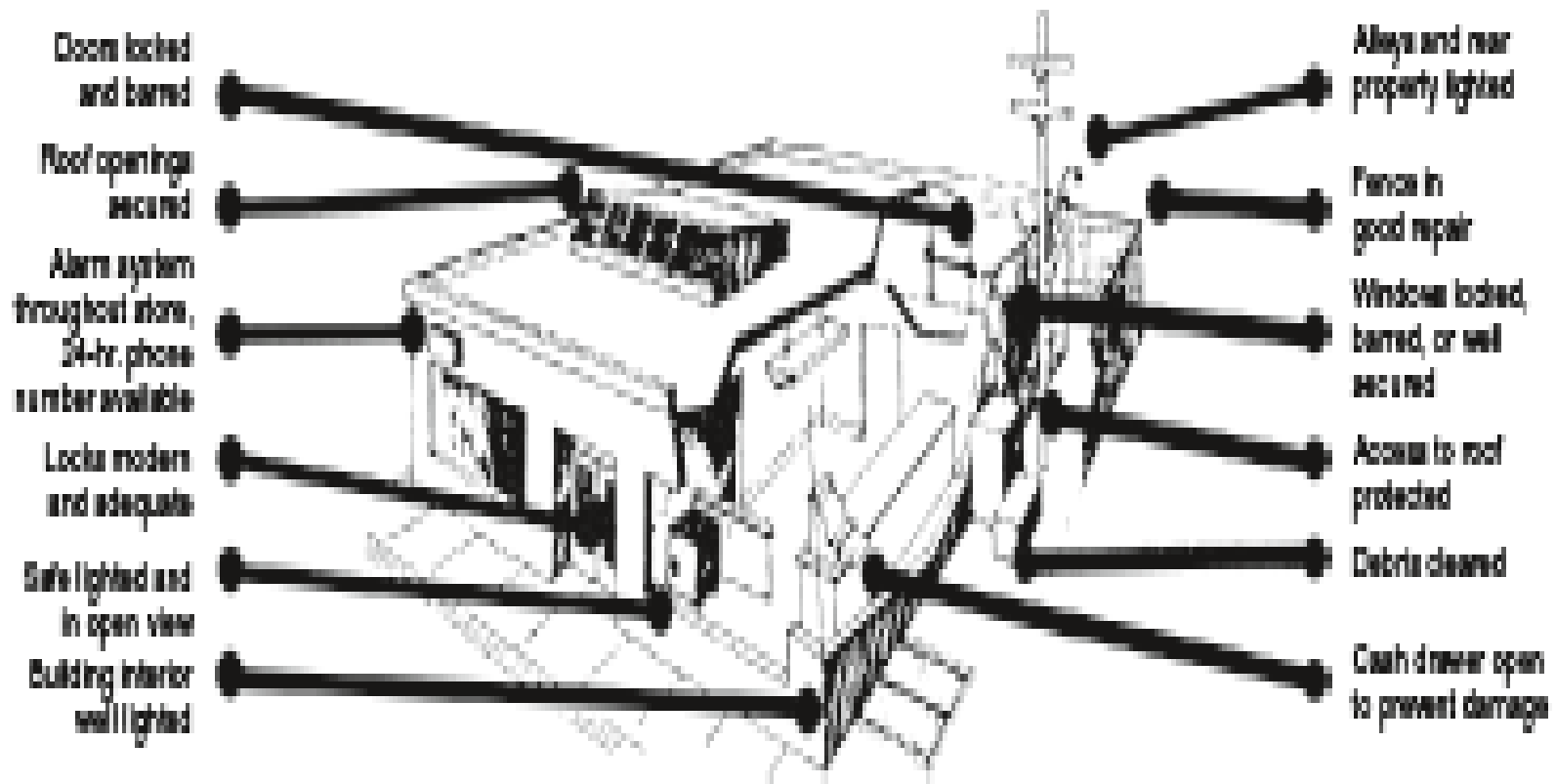
First line of Defense

FIGURE 14-2   Defense around exterior of building.

Two important points to the systems approach

1. *The whole, rather than its individual parts, must be considered.*

2. *Design should allow for an acceptable level of redundancy, without any unnecessary duplication of effort.*

Referred to as system engineering

Security Lighting

Security lighting has three primary objectives:

1. It must act as a deterrent to intruders.

2. It must make detection likely if an intrusion is attempted.

3. It should not unnecessarily expose patrolling personnel.

Four types of lighting systems

Lighting systems are often referred to as:

1. " continuous, "
2. "standby, "
3. " movable "
4. " emergency. "

Types of lighting:

1. Gaseous discharge: street lighting
2. Metal halide (Gaseous): sports arena type lighting
3. Incandescent: home lighting.
4. Quartz: Bright white light.

Four Application considerations

1. When designing a protective lighting system, consider <u>three lines of defense:</u>

    - *the perimeter*
    - *open yards*
    - *building exteriors*

2. All accessible exterior lamp <u>enclosures should be in tamper- or vandal-resistive housing</u>. This means that the receptacle and lens should be constructed of a material that will resist damage if attacked and that the mounting screws or bolts should be tamper-resistant.

Application consideration

3. If protective lighting is to be located in an area that may be subject to explosions, the <u>housings should be explosive-resistant</u>.

4. Before finalizing any decision on the installation of lighting, <u>consider the impact that additional lighting will have on your neighbors</u>. Failure to consult with a neighbor prior to an installation may result in costly redesign.

Glazing

- Safety/fire:

  – Tempered: safety glass several times stronger, when it does break, it disintegrates.

  – Wired: extra strength: for passageways, entrance doors, sliding doors, bathtub enclosures, shower doors.

Tempered Glass
Breakage Pattern

Heat-Strengthened Glass
Breakage Pattern
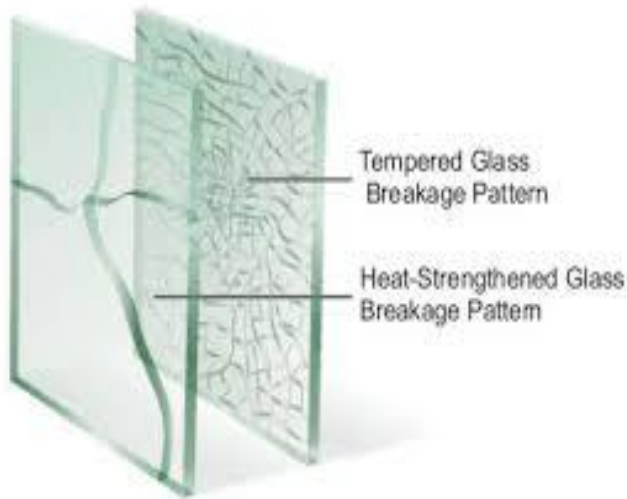
- Burglar/vandal-resistive:
  - Laminated, wired, acrylic, polycarbonate: all much stronger.
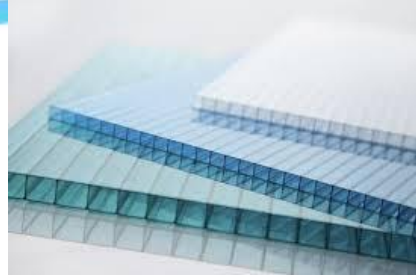
- Bullet resistive: laminated with glass and polycarbonate: banks

- Special purpose   or, coated, heated, and rough or patterned: conf   lighting and privacy.

Intrusion detection

- Every intrusion detection system is meant to detect the following:

  1. Unauthorized entry

  2. Unauthorized movement within

  3. Unauthorized access to controlled areas or objects

- There are three components to an intrusion detection system:

  1. Detectors/sensors

  2. System controls

  3. Signal transmission

Detectors/sensors

- Magnetic switches: door or window contacts
- Metallic foil: narrow strip of metal designed to break.
- Vibration: shock sensors
- Ultrasonic: motion detectors in a enclosed area
- Photoelectric: a beam of light reflected

Detectors/sensors

- Infrared: area detector: measure radiated energy and ambient temperature
- Microwave: high frequency radio waves in a protected area
- Dual technology: combines two technologies
- Video motion: uses motion sensors and CCTV

System controls/monitoring

System controls includes:

1. ***Data Processing Equipment***

2. ***Signal Transmission Equipment***

3. ***On/Off***

4. Reset controls

5. Backup power supply

6. LED indicators

7. Equipment specific to particular systems

System controls/monitoring

System monitoring:

    1. Local: bell or siren

    2. Proprietary: monitored on site

    3. Commercial: monitors several sites.

    ✧*Usually transmitted via phone or internet lines to monitoring site.*

Card Access

Magnetic strip encoding

Minimum capabilities:

- ***Restrict access by authorized persons to certain times and/or days of the week.***
- ***Allow controlled after-hours access to selected areas within.***
- ***Control after-hours access to a parkade.***
- Selectively control after-hours use of elevators.
- Maintain a record of all valid and invalid use of cards.
- Provide an audit trail permitting a printout of persons on the property at any one time.

Card Access

There are numerous types of cards:

- Magnetic coded: credit card
- Magnetic strip coded: credit card
- Proximity coded: contactless
- Weigand coded: slide through a reader
- Hollerith: holes in it
- Optical coded: bar code

Access control and ID cards

- Company name and logo
- Details of cardholder
- Name
- Department
- Date of birth
- Signature
- Photograph
- Condition of use (restrictions)
  - Used widely in government and schools
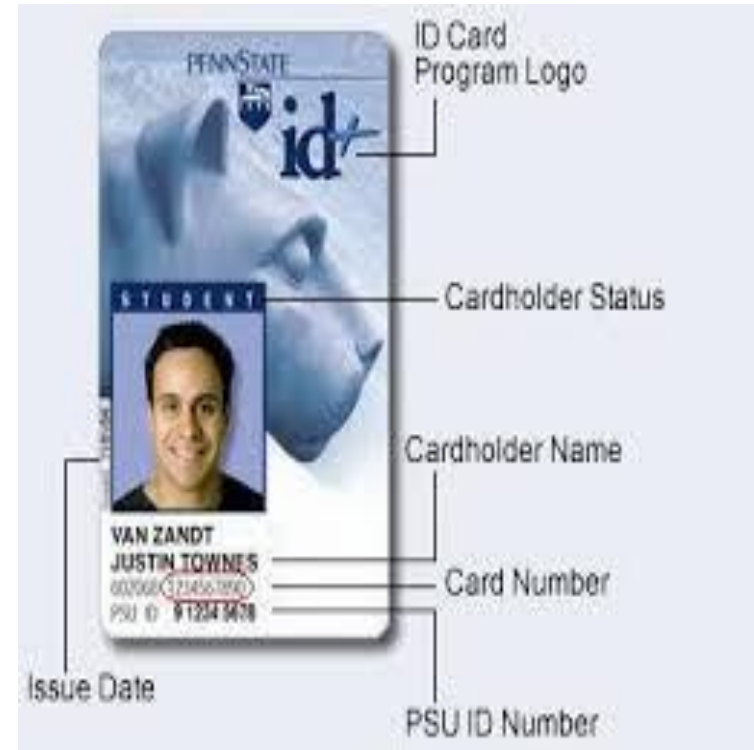
Locking hardware

- Locking hardware can be categorized as mechanical, electrical, or electromagnetic, and as either security or non-security.

- Quality mechanical security locks should be used for all of the following:
  - *Perimeter openings*
  - *Doors that control/restrict internal movement*
  - *Doors to sensitive/restricted areas*

- Only deadbolt locks should be considered. The bolt should offer a minimum of 1-inch throw. If the door is a glass metal-framed door, the bolt should be of the pivotal type to ensure maximum throw.

CCTV

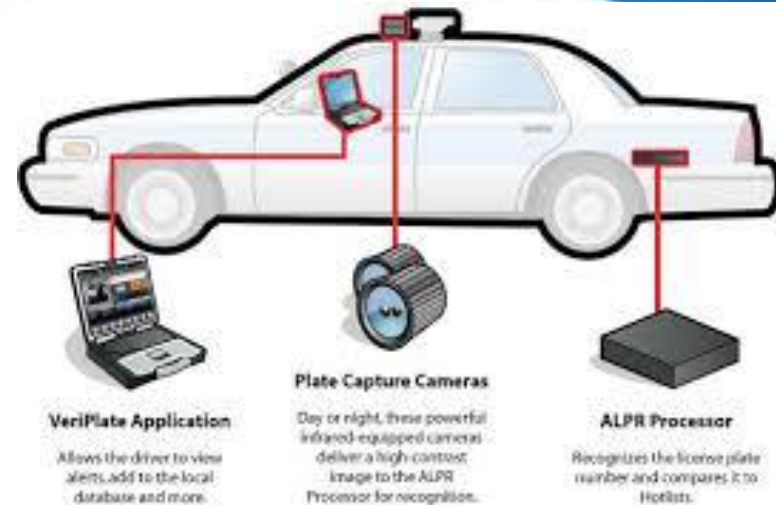CCTV has three major roles in any physical security program:

1. To deter crime or unwanted activities

2. To allow the ability to witness an act as it occurs

3. As an investigative tool after an act has already been committed

There are three main views that a standard CCTV system should provide, depending upon the application requirements:

1. Identification of any subjects
2. Identify the actions within a scene
3. Identify the scene where the act occurred

CCTV FEATURES

- Video motion detection

- People counting and tracking

- Object classification

- License plate recognition

- Facial Recognition

- Crowd Detection   https://www.youtube.com/watch?v=NuYDtonfmUA

- Psychology of motion

- https://www.youtube.com/watch?v=GhzRiIx6Qxw

Plate Capture Cameras

VeriPlate Application
Allows the driver to view alerts add to the local database and more.

Day or night, these powerful infrared-equipped cameras deliver a high-contrast image to the ALPR Processor for recognition.

ALPR Processor
Recognizes the license plate number and compares it to Hotlists.

Components of a CCTV system

- Cameras
  1. *CCD – Charged coupled device*
  2. *CMCS – Complementary metal oxide semiconductor*
- Lenses
  1. *Fixed*
  2. *Varifocal*
  3. *Zoom - https://www.youtube.com/watch?v=8LwwnoaSB5U*
- Housings
- Monitors

Components of a CCTV system

- Sequential switches
  - *Review multiple cameras on one monitor*
- Motion detectors
- Pan/tilt/zoom features
- Controls
- Consoles
- Video recorders
- Day/time generators

Safes and Vaults

- Provide levels of protection against: <u>burglary, robbery and fire</u>.
- Burglary resistive safes:
  - Locks: single comb, single key lock combination and dual combination
  - Interiors: various types of shelving depending upon the asset.
  - Depository: allow deposit without giving access to the interior
  - Time locks: specific time frames.
  - Time Delay locks: even after using combination, still must wait
  - Relocking devices: back up features
  - Extra weight: should be a minimum of 340 kg or 750 lbs.
  - Floor anchoring: bolt to the floor.
- https://www.youtube.com/watch?v=8LwwnoaSB5U

Fire Resistant

- Burglary resistive vaults: if a person can enter it, then it is a vault. Reinforced on all 6 sides.

- Fire resistive containers: insulated safes, filing cabinets, record containers all offer varying degrees of protection from heat. Note they are not burglary resistive as they are made out of different material.

  - Paper up to 350 degrees
  - Tapes and disc 150 degrees

Fencing Rules

History

800 BC – City of Pompeii

Great Wall of China:1368-1644

Barbed Wire: 1867

Chain Link: 1800 in the UK

1. Minimum of 7 feet in height excluding top overhang.
2. 9-gauge or heavier.
3. Mesh openings must not be larger than 2" square inches.
4. Fabric must be fastened securely to rigid metal or reinforced concrete posts set in concrete.
5. No more than 2 inches between the bottom of the fence and the ground.
6. Fabric extend below the surface.

Fencing Rules

7. Top overhang should face outward and upward at a **45-degree angle.**

8. Overhang supporting arms should be firmly affixed to the top of the fence posts.

9. **Overhang** should increase the **overall height** of the fence **by 1 foot**.

10. Three strands of barbed wire, **spaced 6 inches** apart, should be installed on the supporting arms.

11. A clear zone of **20 feet** or more should exist between the perimeter and exterior structures.

12. Where possible, a clear zone of **50 feet** or more should exist between the perimeter barrier and structures within the protected area.

Fencing

- First and foremost a barrier

- Only a delay system

- Supplement with sensors, detectors or CCTV

Convergence

- The meshing of physical security, logical security, information technology, risk management, and business continuity into a seamless and integrated system and process.

Education

1. Career planning
2. Employers are searching for dedicated security officers
3. Work exposure is critical
4. Professional designations
   - ASIS
   - IFPO

Closure

- Define physical security planning.
- List the five steps in the security planning process.
- List the three options for intrusion monitoring.
- Explain the three objectives of security lighting.
- Name different types of locking hardware
- Provide the three roles of CCTV and access control.
- Identify the correct height for security fencing
- Explain the fire safe temperature for paper
- Explain what convergence is
- Conduct a facility tour to explain to the class the physical security measures present.

Class assignment

Students are to go out in groups and make a detailed list of all the physical security measures in place at the training facility. You have 45 minutes to complete the assignment.

Items needed:

- Clip Board

- CPTED Assessment

- Writing tool

Review

- What are the five steps in the security planning process?

1. Assets are identified.

2. Loss events are exposed.
    - Industrial disasters
    - Natural disasters
    - Civil disturbance
    - Crime
    - Other threats

3. Occurrence probability factors are assigned.

4. Impact of occurrence is assessed.

5. Countermeasures are selected.

Review

- What are the three options for intrusion monitoring?
- Every intrusion detection system is meant to detect the following:

   1. Unauthorized entry
   2. Unauthorized movement within
   3. Unauthorized access to controlled areas or objects

- There are three components to an intrusion detection system:

   1. Detectors/sensors
   2. System controls
   3. Signal transmission

Review

- What are the three objectives of security lighting?

Security lighting has three primary objectives:

    1. It must act as a <u>deterrent</u> to intruders.

    2. It must make <u>detection</u> likely if an intrusion is attempted.

    3. It should <u>not</u> unnecessarily <u>expose patrolling personnel</u>.

Review

- What are the three roles of CCTV and access control?

- CCTV has three major roles in any physical security program:
    1. To deter crime or unwanted activities
    2. To allow the ability to witness an act as it occurs
    3. As an investigative tool after an act has already been committed

- Every intrusion detection system is meant to detect:
    1. Unauthorized entry
    2. Unauthorized movement within
    3. Unauthorized access to controlled areas or objects

Questions?

Review for the quiz