Physical (Environmental) Security

Domain 10

Overview

The Physical (Environmental) Security domain is a comprehensive evaluation of physical, environmental, and procedural risks that may exist within a facility, organization, or structure in which information systems are stored and managed.

Key Areas of Knowledge

- **Understand site and facility design considerations**
- **Support the implementation and operation of perimeter security (e.g., physical access control and monitoring, audit trails/access logs)**
- **Support the implementation and operation of internal security (e.g., escort requirements/visitor control, keys and locks)**
- **Support the implementation and operation of facilities security (e.g., technology convergence)**
  - Communications and server rooms
  - Restricted and work areas security
  - Data center security
  - Utilities and Heating, Ventilation and Air-Conditioning (HVAC) considerations
  - Water issues (e.g., leakage, flooding)
  - Fire prevention, detection and suppression
- **Support the protection and securing of equipment**
- **Understand personnel privacy and safety (e.g., duress, travel, monitoring)**

Agenda

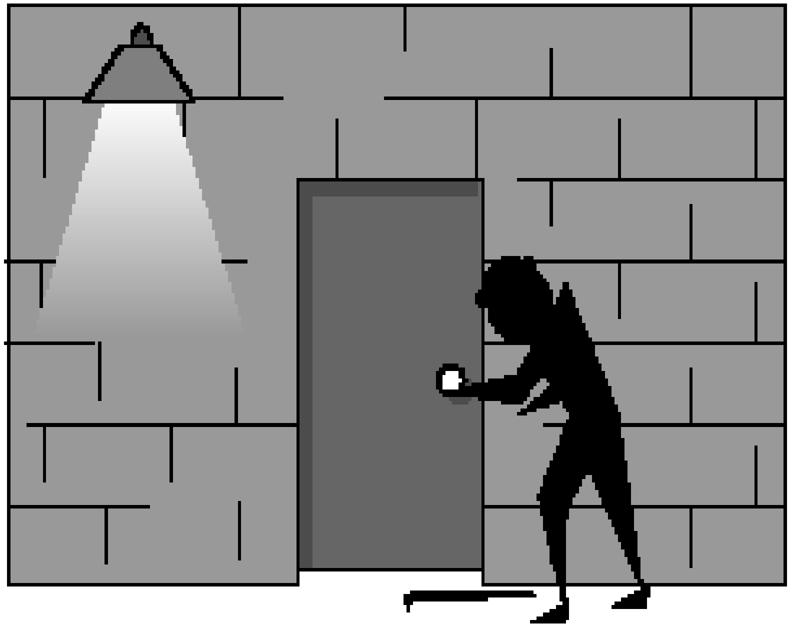
- **Understand site and facility design considerations**
- Support the implementation and operation of perimeter security (e.g., physical access control and monitoring, audit trails/access logs)
- Support the implementation and operation of internal security (e.g., escort requirements/visitor control, keys and locks)
- Support the implementation and operation of facilities security (e.g., technology convergence)
- Support the protection and securing of equipment
- Understand personnel privacy and safety (e.g., duress, travel, monitoring)

Another Approach to Security

Hacker

Computer Security

Intruder



Physical Security

Physical Security Design Considerations

- **Facility - Site Location**
- **Facility - Layered Defense**
  - Outer Perimeter
  - Building Grounds and Construction
  - Ingress/Egress
  - Interior
- **Mobile computing**
- **Home workers**

Physical Security Components

- **Physical – First Line of Defense**
  - Perimeter Protection
    - Surroundings (terrain, remoteness, etc.)
    - Structural (fences, bollards, walls, gates, etc.)
  - Building structure
- **Technical Controls**
  - Proximity devices
  - Intrusion detection systems
- **Supporting Facility Controls**
  - Electrical power
  - Heating, ventilation, air conditioning
  - Fire detection and suppression

Mentality Approaches

- “Fortress mentality” does not implement layers of protection
- The first step in designing and effectiveness physical security program begins with the identification of the physical security program team.
- Physical security measures are the first line of defense and people are the last line of defense

Facility Location

- **Location Considerations**
  - Natural disasters
  - Proximity to highways, airports, a military base, etc.
- **Hazards**
  - Joint tenants
  - Vandals & burglars
- **Outside Assistance**
  - Police, fire, medical
  - Public services
- **Visibility**
  - Line of sight
  - Markings

External Boundary Protection

Fences and Walls

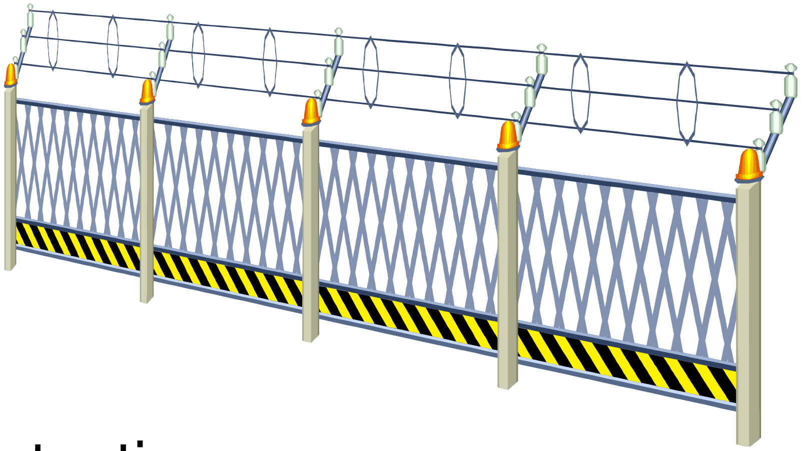
- Crowd control, deter trespassers, control access to entry points
- Can be costly and unsightly
- Will not stop a determined intruder

Bollards

- Permanent or retractable posts to control traffic and protect property
- Placement should protect facility from vehicles ramming into it
- Between a parking lot or street and the building
- Large concrete planters can provide the same protection

External Boundary Protection

Fencing



- Controls entrance access
- Can be costly and unsightly
- Heights provide degrees of protection
  - 3-4 feet – deters casual trespassers
  - 6-7 feet – too high to climb easily
  - 8 feet with 3 strands of barbed wire – deter determined intruder
- Critical areas should have at least 8-foot fences

External Boundary Protection

PIDAS Fencing

- Perimeter Intrusion Detection and Assessment System
- Detects if someone tries to climb a fence or damage the fence
- Mesh-wire fence with a passive cable vibration sensor that sets off an alarm if detected

Perimeter Walls

- Reinforced concrete or solid brick
- Not less than 10 feet
- Can have barbed wire or spikes on top

External Boundary Protection

- **Gates**
  - Equivalent standard to a fence or wall
  - Strong hinges to resist tampering
  - Manned or CCTV monitoring
- **Lighting**
  - Discourage intruders and protect personnel
  - Entrances and parking lots
    - At least 8 ft. high providing at least 2 foot-candles
    - NIST recommendation
  - Provides detection and deterrence

Facility Construction

- **Business needs and required protection levels**
  - Company that sells baseball cards versus missiles

- **Physical construction materials aid in overall protection of the facility**
  - Crime Prevention Through Environmental Design (CPTED)
  - Protection against vandals, fire, natural disasters
  - Physical characteristics of a building determine how easy it is to conduct electronic surveillance on sensitive areas

- **Use of the facility will determine codes and regulations**
  - People will be working in it versus just storage of equipment/ paper

Facility Attributes

Internal Walls

- Combustibility of material (wood, steel, concrete)
- Fire rating
- Reinforcements for secured areas

Ceilings

- Combustibility of material (wood, steel, concrete)
- Fire rating
- Load and weight bearing rating
- Drop ceiling considerations

Facility Attributes - Windows

- Tempered glass should be considered over plate glass
  - Plate glass shatters producing jagged shards
- Acrylic (Plexiglas®) windows easily scratch, become hazy, and give of toxic fumes when burning
- Polycarbonate (Lexan®) windows combine the best of glass and acrylic, and in the right thickness, can be anti-ballistic
- Windows and equipment should be positioned to resist shoulder surfing and damage from direct sunlight
- Windows that open should be alarmed
  - Other security measures like those applied to doors may be required if the window could possibly be used as an entry point

Facility Attributes – Doors

- **Fire Rating should be the same as walls**
- **Resistance to forcible entry**
  - Solid core to protect from breach and add a barrier for fire
  - Directional opening – should not open out unless required by code; doors that open out must have sealed hinge pins to resist compromise
  - Door frames need to be connected to wall studs to resist force
  - Doors affixed to the frame with a minimum of 3 secure hinges
- **Some doors may need to be monitored and/or alarmed**
  - Emergency exit doors must be marked and include panic bars
- **Electric door locks may need to revert to a disabled state if a power outage occurs for safe evacuation**
- **Lighted doorways provide for security (a deterrent) and safety**

Facility Attributes

Heating and Air Conditioning

- Positive air pressure
- Protected intake vents
- Dedicated power lines
- Emergency switch-off valves
- Placement
- Threat: Overheating/Overcooling

Environmental Considerations – HVAC

- **Maintain proper temperature**
  - 70-74º F / 20-22º C
- **Maintain proper humidity**
  - 45-60% for safe data processing
  - Hygrometer used to monitor humidity
- **High humidity**
  - Can cause corrosion
- **Low humidity**
  - Can cause static electricity

Static Electricity Prevention

- Use anti-static flooring in data processing areas
- Ensure proper humidity
- Have proper grounding of building and outlets
- Do not have carpeting in data centers or have static-free carpets if necessary
- Wear anti-static bands when working inside of computer systems

HVAC

During Fire

- HVAC should be turned off so that smoke is not spread and fire is not provided with more oxygen

Positive Pressurization

- Air goes out an open door instead of in
- In a fire situation, smoke must go out of the building

Control Contaminants

- Concentration of certain gasses can accelerate corrosion and negatively affect device components
- Dust can affect computer hardware

Facility Attributes

Power Supplies

- Backup and alternate power supplies
- Clean power source
- Dedicated feeders to required areas
- Placement and access to distribution panels and circuit breakers

Water and Gas Lines

- Shutoff valves
- Positive flow (material should flow out of building, not in)
- Placement
- Threat: Flood/ Explosion

Computing Area Location

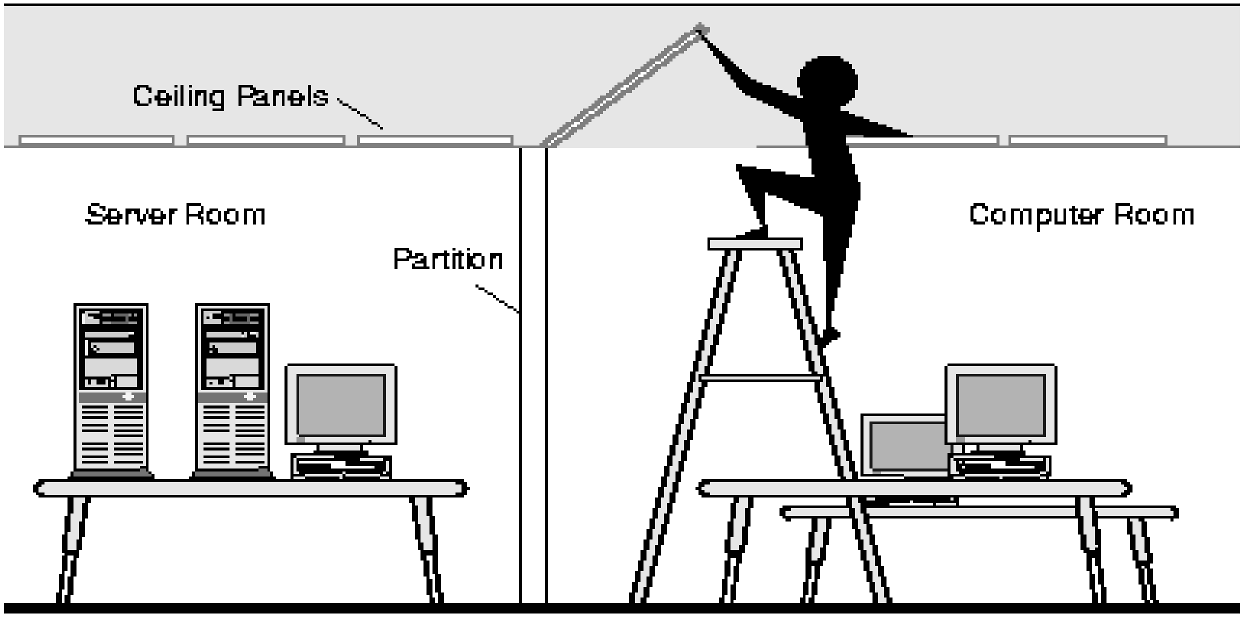
- Should not be on top floor in case of fire
- Should not be in basement in case of flood
- Should not be on first floor to control access
- Should not be located next to stairs, bathrooms or elevators
- Located in core of facility for protection from exterior threats

Sensitive Room Characteristics

- **Should have no more than two doors**
  - Small windows and restricted amount of windows
- **Full-height walls**
- **Walls, doors, ceiling must have the same rating and at least a one-hour minimum fire rating**
  - Adjacent walls where paper records are stored must have a two-hour fire rating

Internal Partitions

- **Internal partitions should not be used as a security mechanism to protect sensitive areas**



Agenda

- Understand site and facility design considerations
- **Support the implementation and operation of perimeter security (e.g., physical access control and monitoring, audit trails/access logs)**
- Support the implementation and operation of internal security (e.g., escort requirements/visitor control, keys and locks)
- Support the implementation and operation of facilities security (e.g., technology convergence)
- Support the protection and securing of equipment
- Understand personnel privacy and safety (e.g., duress, travel, monitoring)

Physical Security Controls

- Locks
- Physical IDS
- Access Logs
- Background Checks
- Separation of Duties, Job Rotation, Mandatory Vacations
- Awareness Programs
- Screen Filters
- Proper Disposal Procedures
- Guards
- Smoke Detection and Suppression Systems
- Controlled Physical Access like Turnstiles and Man-Traps

Physical Security Controls

- **Required by law or regulation**
  - No option on implementation
  - Fire exit doors with panic bars and exit lights

- **Low cost but high benefit**
  - Cost of control is low and provides a high level of protection
    - Door lock
    - Employee awareness – questioning suspicious individuals

- **Cost/Benefit**
  - Benefit of control outweighs its cost
    - Potential loss is higher than cost of control

Monitoring with Closed Circuit TV

- **Requirements**
  - Detection, recognition, identification
  - The “focal length” of a lens defines its effectiveness in viewing objects from a horizontal and vertical view.
    - Short focal length = wider angle views
    - long focal length = narrower views
- **Connected to a recording and/or monitoring station**
  - Transmission medium: wired or wireless
  - Lighting (need to be able to contrast between objects and background)
  - Blind spots; lens requirements (includes the height, depth and width)
  - Number of cameras; normal aspect ratio is 4:3 (horizontal:vertical)
- **Considerations**
  - Workplace privacy issues
  - Virtual CCTV

Facility Access

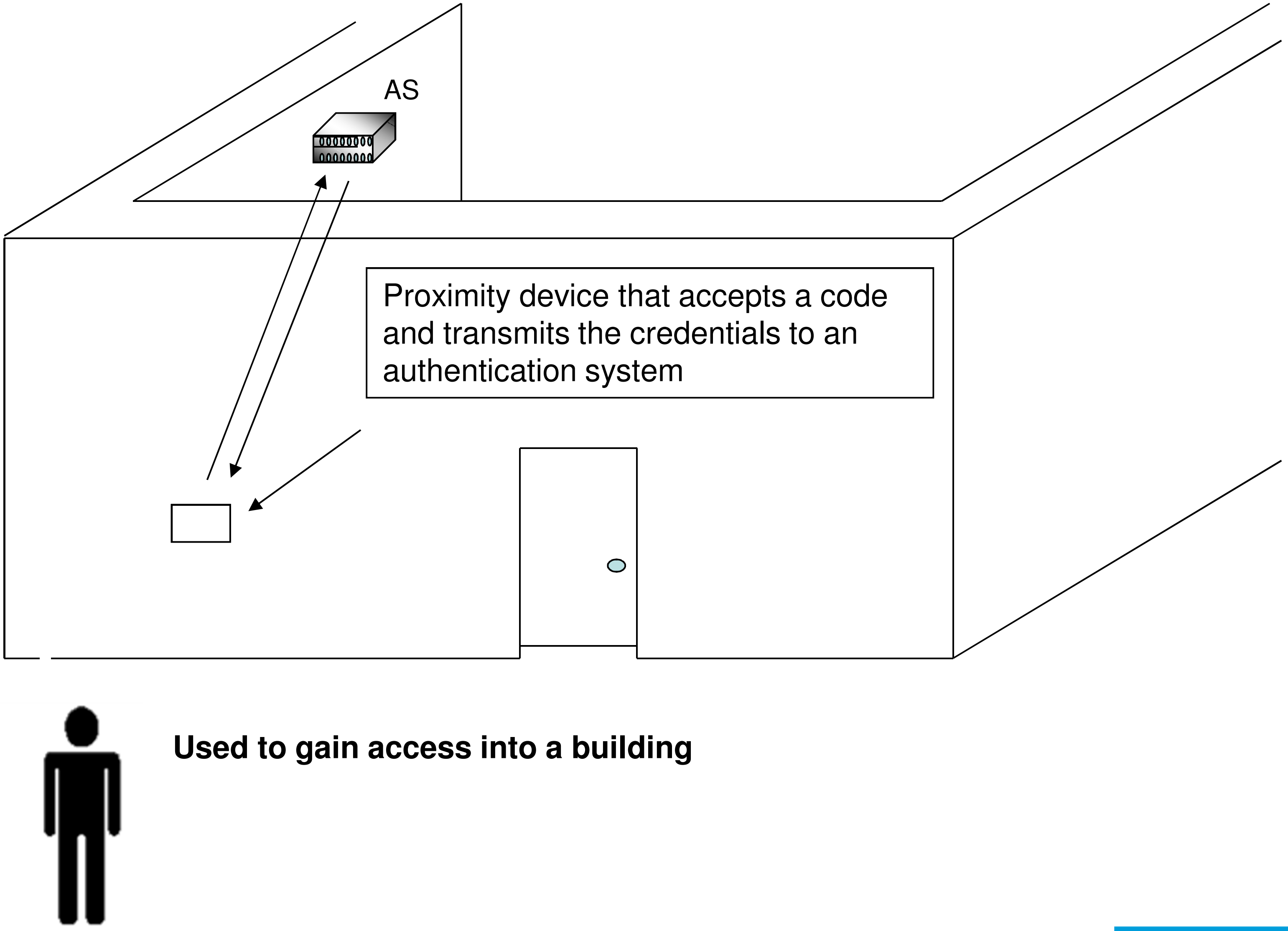
Identification Mechanisms

- Photo ID for a security guard
- Biometric devices
- Card badge reader – swipe systems
  - Magnetic stripe
  - Embedded wire
  - Magnetic dot
  - Bar code – optical

Facility Access

- **Types of Proximity Devices:**
- **User activated**
  - Wireless keypad
  - User keys in a code that is sent over air waves to the reader
- **Passive systems**
  - No batteries, powered by sensor
  - simple circuits transmit a code
- **System sensing/ Radio Frequency ID**
  - Reader transmits interrogating signal and user device sends access code
  - Also called transponder devices

Proximity Device



Proximity device that accepts a code and transmits the credentials to an authentication system

Used to gain access into a building

Entrance Protection

Turnstiles

- Revolving doors that can be activated to “lock” and not allow unauthorized individuals to enter or leave facility

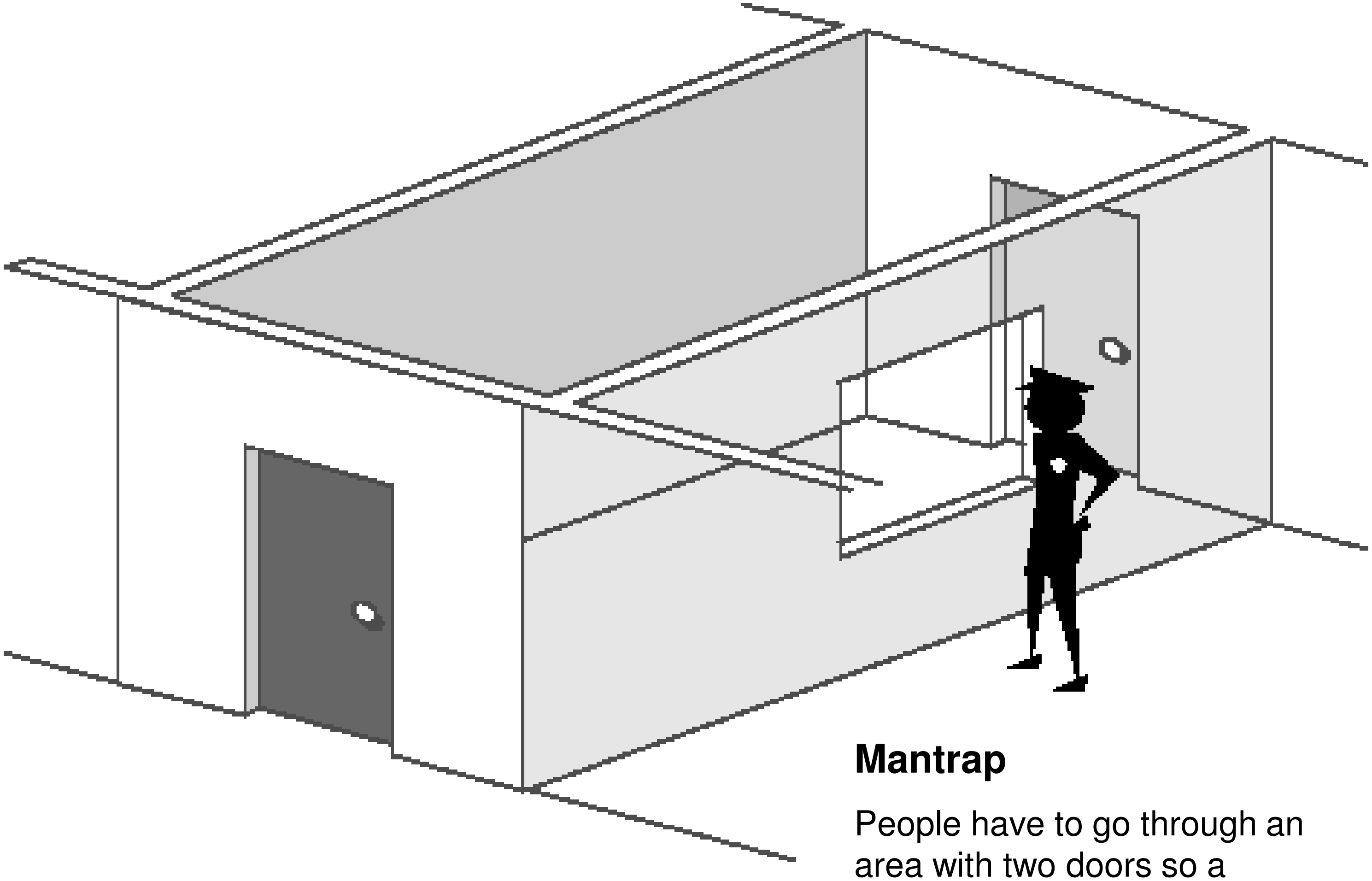
Mantraps

- Routing people through two stationary doorways

During an emergency consider

- Fail-soft (door defaults to being unlocked)
- Fail-secure (door defaults to being locked)
- Fail-safe (door defaults to a state that protects life)

Mantrap



Mantrap

People have to go through an area with two doors so a guard can check credentials

Security Guards Functions

- **Deter and correct improper actions**
- **Checking credentials at entry points**
- **Ensuring company property does not leave facility**
- **Enforce regulations**
- **Monitor intrusion detection and fire alarm systems**
- **Watching for suspicious activity**
    - Watch for piggybacking
- **Verify doors and windows are locked**
    - Should not stay stationary
    - May have a post and one roving guard
- **Personnel is the most expensive countermeasure to reduce physical security risks**
- **Increased liability**

Access Logging

Tracking Who Comes and Goes

- Access logs should be used to track who enters and leaves facilities if that level of protection is necessary
- Usually a security guard maintains these logs
  - Check Identification
  - Photograph visitors and assign temporary badge
- Not a preventative control, but a detective control
  - Logs can be collected and maintained in hard copy, computerized, and/ or CCTV recording
- Should capture who came in, when, what department they were to visit, who signed responsibility for them and escorted them, and what time they left

Agenda

- Understand site and facility design considerations
- Support the implementation and operation of perimeter security (e.g., physical access control and monitoring, audit trails/access logs)
- **Support the implementation and operation of internal security (e.g., escort requirements/visitor control, keys and locks)**
- Support the implementation and operation of facilities security (e.g., technology convergence)
- Support the protection and securing of equipment
- Understand personnel privacy and safety (e.g., duress, travel, monitoring)

Lock Types

- **Three primary lock types:**
  - Something you have – Key
  - Something you know – Combination
  - Something you are - Biometric

- **Conventional Locks**
  - Locks easily picked/ bumped and keys easily duplicated
  - Control and distribution of keys can be a problem

- **Pick and bump resistant Locks**
  - Higher cost
  - Harder to pick/ bumped and keys not as easily duplicated
  - Distribution and control still a problem

Lock Types

Electronic Combination Lock (aka Cipher Lock)

- A keypad for a combination
- Combinations change at least every 12 months, when an employee leaves, or when possible compromise

Key Card Systems

- Cards encoded with an access code
- High-end systems can allow control of when people are authorized to enter, log entrances and exits, and control a group of doors – not just a single door

Biometric Systems

- Provide identification and similar functionality to key card systems

Personnel Access Control

- **Cipher locks (keyless lock)**
  - Programmable locks with keypads
  - Combination lock
  - Door delay – If a door is held open for a long period of time, an alarm will trigger to alert personnel of suspicious activity
  - Key-override – A specific combination can be programmed to be used in emergency situations to override usual procedures or for supervisory overrides
  - Master-keying – This option enables supervisory personnel to change access codes and other features of the cipher lock
  - Hostage alarm – If an individual is in duress and/or held hostage,
    there can be a combination he or she enters to communicate this
    situation to the guard station and/or police station

Best Practices for Entry Controls – 1 of 2

- Limit number of entrances to facility and computer rooms
- Doors should resist forced entry
- Screening device at every entrance
- Log entries and exits
- Watch for property leaving facility

Best Practices for Entry Controls – 2 of 2

- Secure all openings
- After an unusual diversion (bomb threat, power outage, false fire alarm) search facility
- After suspicious activity, review logs
- Do unscheduled inspections

Agenda

- Understand site and facility design considerations
- Support the implementation and operation of perimeter security (e.g., physical access control and monitoring, audit trails/access logs)
- Support the implementation and operation of internal security (e.g., escort requirements/visitor control, keys and locks)
- **Support the implementation and operation of facilities security (e.g., technology convergence)**
- Support the protection and securing of equipment
- Understand personnel privacy and safety (e.g., duress, travel, monitoring)

Intrusion Detection Systems

Definition

- Process of identifying attempts to penetrate a system or building with the goal of gaining unauthorized access
- The system can include sensors, control units, transmission line and display monitoring units

Activation

- System should be activated by a primary and alternate employee when employees leave for the day
- Whoever is monitoring system should have contact names of who to call if alarm sounds

Two Main Types of Systems

Electro-mechanical

- Magnetic switches
- Metallic foil in windows
- Pressure mats
- Most widely used

Volumetric

- Vibration
- Microwave, ultrasonic, passive infrared
- Photo-electronic
- Not used as often

Types of Electro-mechanical Systems

Contact Sensor

- Electrical circuit is broken
- Opening a door or window

Pressure Mat Sensor

- Intruder steps on mat

Closed-circuit

- Electrical circuit is broken
- Cutting a wire or breaking a window

Types of Volumetric Systems

- **Proximity**
  - Emits magnetic field and monitors that electronic field
  - Detects approaching or presence of object
  - Many false alarms because of sensitivity, thus should be a backup device and not primary security control
- **Photoelectric**
  - Passive device sensitive to a change in an area’s light level
  - Only used in windowless areas
- **Video Motion Detector**
  - Movement picked up on video camera
  - Added value of providing an audit trail with recorded footage

Motion Detector Devices

- **Uses Doppler effect**
- **Source of sound or electromagnetic signal moves towards or away from a receiver, the frequency of the signal will be higher or lower**
- **Motion is detected by change in frequencies**
- **Detects slight difference in frequency of source and sounds an alarm**
  - Sonic detection: audible range (1,500 to 2,000 hertz)
  - Ultrasonic detection: High-frequency (19,000-20,000 hertz)
  - Microwave detection: Higher frequencies (400-10,000 megahertz)

Acoustical-Seismic Detector Devices

- Detect vibrations
- Microphones are used to detect sounds above the ambient noise level in the protected area
- Can be set off by storms, aircraft, rain, etc.

Intrusion Detection System Characteristics

- Expensive
- Requires human intervention
- Redundant power supply and emergency backup power
- Can be linked to a central security system
  - Fire and intruder detection
- Should fail-safe

Intrusion Detection System Precautions

- Be resistant to and detect tampering
- Must be linked to centralized security guard area and local police station
- Can cause a large amount of false alarms
- May be practical when a fence cannot be installed
- Can be penetrated

Agenda

- Understand site and facility design considerations
- Support the implementation and operation of perimeter security (e.g., physical access control and monitoring, audit trails/access logs)
- Support the implementation and operation of internal security (e.g., escort requirements/visitor control, keys and locks)
- Support the implementation and operation of facilities security (e.g., technology convergence)
- **Support the protection and securing of equipment**
- Understand personnel privacy and safety (e.g., duress, travel, monitoring)

Electrical Power

- **Primary Power Source**
  - Provides day-to-day power
  - Dedicated feeders from utility sub-station
- **Alternate Power Source**
  - Backup power in the event of a failure of the primary source
  - Generator
  - Uninterruptible Power Supply (UPS)
    - Inline UPS – constantly provides power from its inverter even when power line is functioning properly
    - Standby UPS – monitors power line and switches to battery power when problem detected
  - Another feeder from a utility sub-station

Uninterruptible Power Supply

Issues to Consider

- Size of load UPS can support
- How long it can support this load (battery duration)
- Speed the UPS takes on the load when the primary power source fails
- Physical space required

Desirable Features

- Long battery life
- Remote diagnostic software
- Surge protection and line conditioning
- EMI/RFI filters to prevent data errors caused by electrical noise
- High MTBF values
- Allow for automatic shutdown of system

Electrical Issues

- Power from the utility feeder is not always consistent and clean

- Power problems can cause hardware to degrade and data loss

- Any device that generates an electromagnetic field in a radio frequency spectrum has the potential to disrupt the operation of other devices in the local area

Electrical Interference

Clean Power is the goal

- Power supply has no interference or voltage fluctuation

Electromagnetic Interference (EMI)

- Line noise
- Caused by difference between wires (hot, neutral, ground)
  - Incorrect wiring – neutral wire is at a different potential than ground wire
- Caused by lightning or electrical motors

Electrical Interference

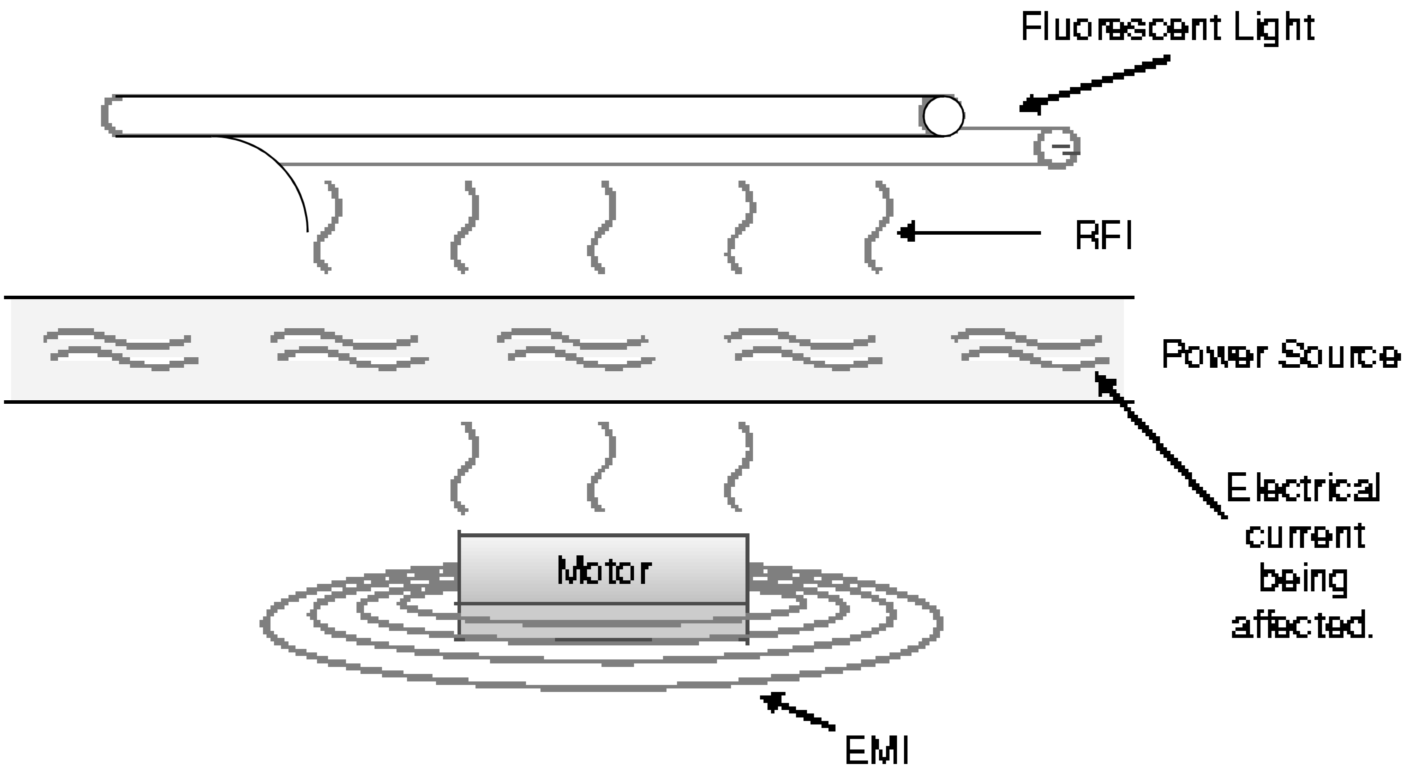
Radio Frequency Interference (RFI)

- Line noise
- Fluorescent lighting, electric cables, components within an electrical system, radio signals

Transient Noise

- Disturbance imposed on a power line
- Can damage devices, corrupt data, hurt people

EMI and RFI Sources



Power Issues

Power Excess

- Spike – Momentary high voltage
- Surge – Prolonged high voltage

Power Loss

- Fault – Momentary power out
- Blackout – Prolonged loss of power

Power Degradation

- Sag – Momentary low voltage
- Brownout – Prolonged power supply that is below normal voltage

Power Preventative Measures

- Voltage regulator
- Line conditioner
- Surge protector
  - Protect from voltage fluctuations
- Power line monitors
  - Detect frequency and voltage amplitude changes
- Shutting down devices in an orderly fashion

Power Preventative Measures

- Connections need to be grounded from the device
to the earth

- Protection from magnetic induction should be
provided through shielded lines
  - Shield long cable runs

- UPS or Generators
  - Backup power supply

Power Preventative Measures

- Use three-prong connections and adapters if using two-prong cables
- Do not plug outlet strips and extension cords into each other
- Do not have power or data lines close to engines or other devices that can cause interference
- Avoid fluorescent lights if possible

Starting Fires

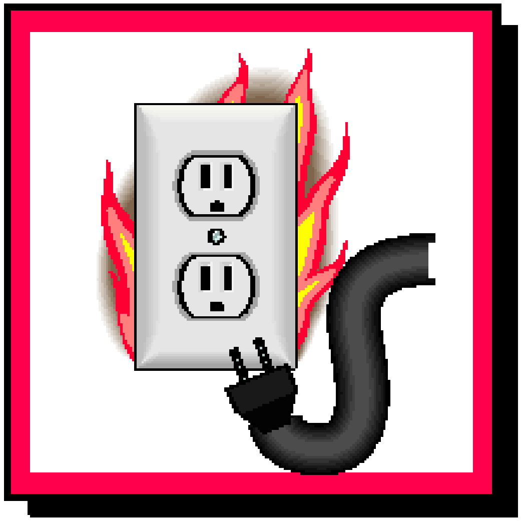
- **High Temperature**
  - Something raised the temperature to cause things to ignite
- **Fuel**
  - What is actually burning (wood, paper, wiring)
- **Four Legs of a Fire**
  - Heat, fuel, oxygen, chemical reaction
- **Fire Extinguishments**
  - Reducing temperature
  - Removing fuel
  - Disrupting chemical combustion
  - Removing oxygen

Approach to Fire Safety

- Balanced approach to design and implementation is necessary to protect personnel and equipment
- Compliance with national and local fire standards increases overall safety
- Prevalent cause of fire in a computing center is electrical distribution systems

Fire Prevention

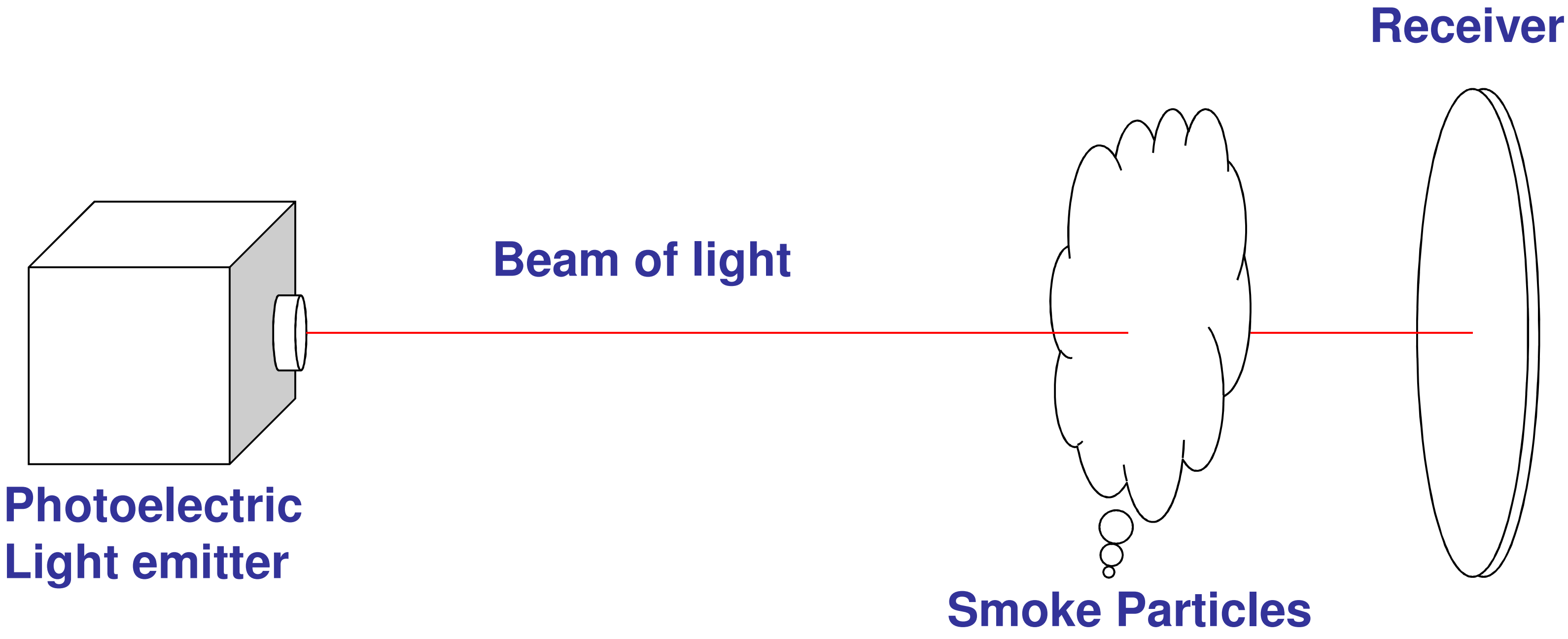
- Building construction
- Safety procedures
- Training employees
- Housekeeping – supplies and combustibles



Automatic Detector Mechanisms

- **Ionization Detector**
  - Reacts to charged particles of smoke
  - Gives early warning
- **Thermal Detector**
  - Alarms when there is a change in temperature – high heat
  - Fixed or rate-of-rise temperature sensors
- **Photoelectric Smoke Detector**
  - Alarms with source of light interrupted
  - Optical detectors sound alarm when light beam is blocked by smoke
- **Infrared Flame Detector**
  - Reacts to emissions of flames
  - Senses pulsation of flame

Photoelectric Smoke Detector



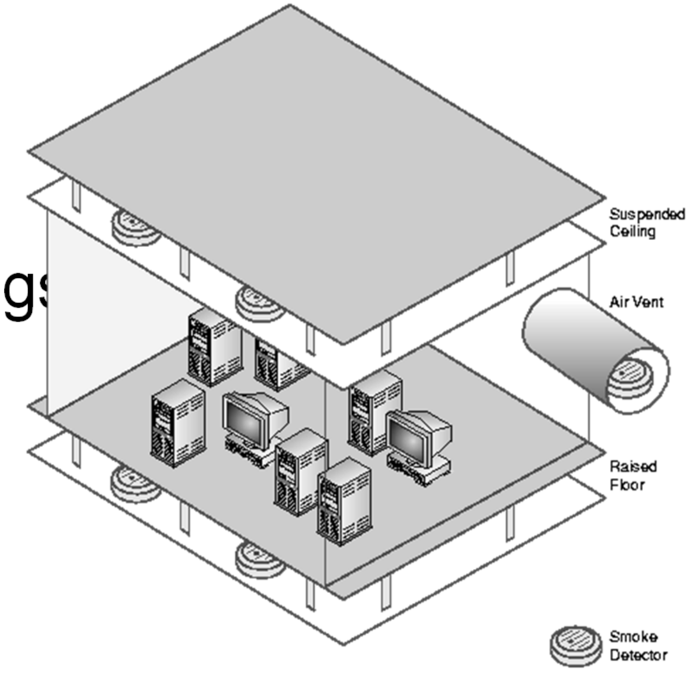
Fire Detection

Fire Detection System

- Can be configured to call a fire station with a pre-recorded message
- Shutdown HVAC system

Detector Placement

- On and above suspended ceilings
- Below raised floors
- In air ducts



Fire Types

CLASS	TYPE	ELEMENTS	SUPPRESSION
Class A	Common Combustibles	Wood, paper, cloth, plastics	Water, soda acid
Class B	Liquid	Petroleum, tars, oils, solvents, alcohol, gases	CO_2, FM-200, Argon
Class C	Electrical	Electrical Equipment, circuits and wires	Gas (Halon) or CO_2. Non-conductive extinguishing agent
Class D	Flammable	Sodium, potassium, etc.	Dry Powder
Class K	Kitchen	Vegetable or animal oils and fats	Wet Chemicals

Suppression Methods

Combustion Elements	Suppression Methods	How Suppression Works
Fuel	Soda acid	Releases CO_2 – displacing oxygen
Oxygen	CO_2	Displaces oxygen
Temperature	Water	Reduces temperature
Chemical Combustion	Halon replacements - FM-200, Inergen, etc.	Interferes with the chemical reactions between elements / displaces oxygen

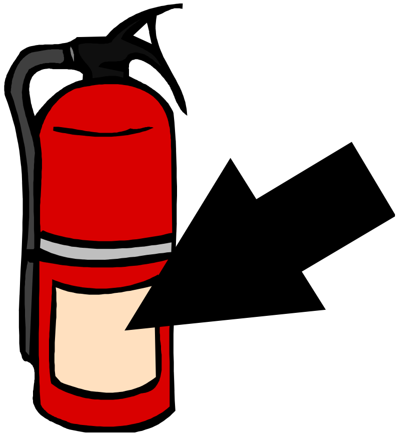
Fire Extinguishers

Halogenated Fire Extinguishers

- Used so that equipment is not damaged by water
- FM-200, FE-13, Inergen

Replacements for Halon without ozone depleting chemicals

- It uses chemicals instead of water



Fire Extinguishers

Carbon Dioxide

- Does not leave residue after use, does not cause damage to sensitive devices
- Can suffocate people

Dry Chemicals

- Not effective against electrical fires

Issues With Different Extinguishers

Carbon Dioxide

- Displaces oxygen
- Colorless and odorless
- Can result in loss of consciousness/death
  - Best used for unattended facilities
  - Delay system in manned areas before distribution

Extinguishers not rated for Class C

- Can cause shock hazard if used on fires involving energized electrical equipment

Halon

- Halogenated extinguishing agent
- Stopped production in 1994 because it depletes the ozone
  - The Montreal Protocol
- FM-200 and Inergen are popular alternatives for chemical-based suppression agents

Water Pipe Types – 1 of 2

- **Wet Pipe**
  - Always contains water
  - Usually discharged at predefined temperature
  - Pipes can freeze and break
  - Can cause water leakage
  - Most commonly used

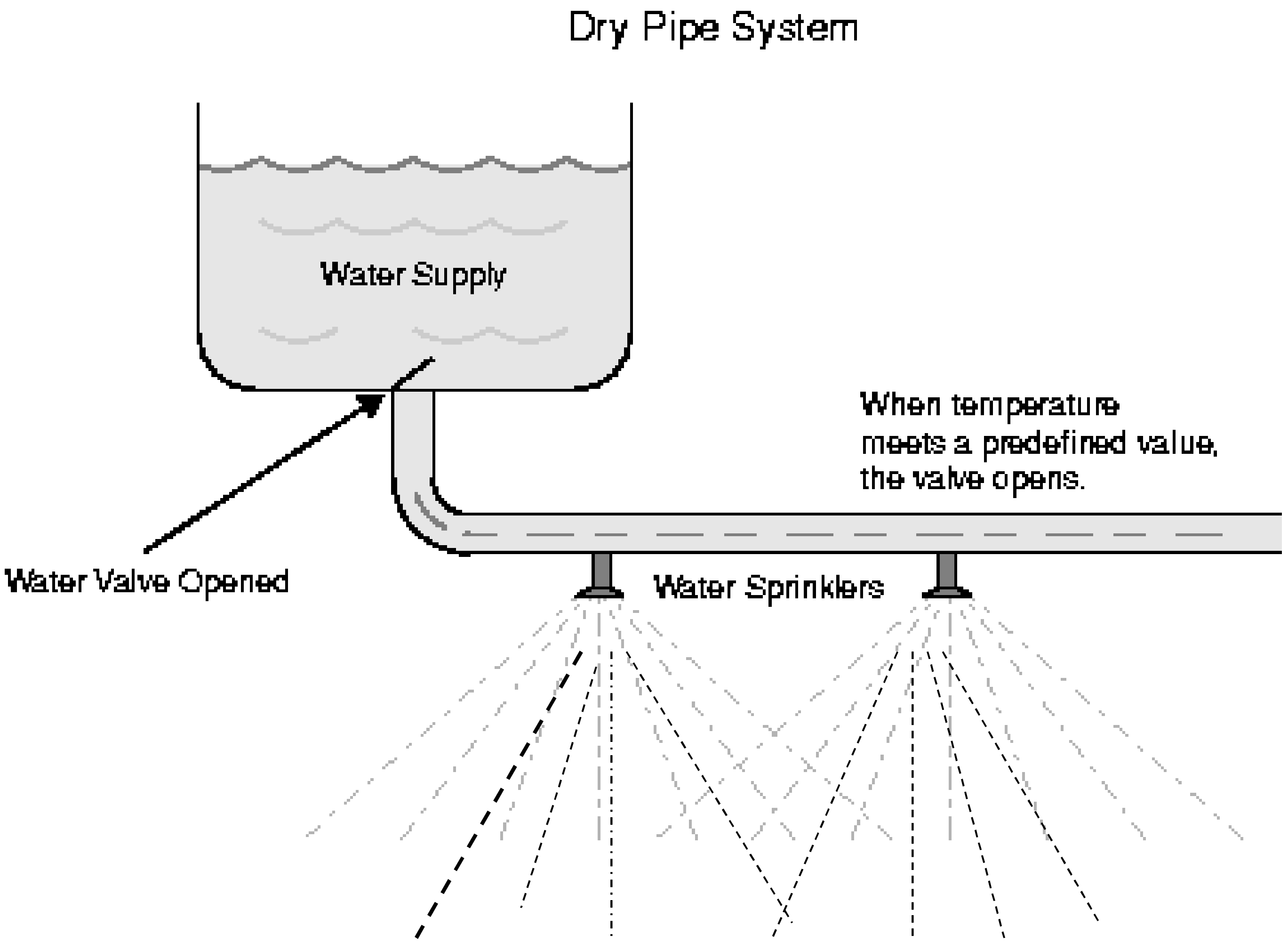
- **Dry Pipe**
  - Water not in pipe
  - Release after a delay
  - Allows someone to shutdown system before release of water
  - Pipes will not freeze and break – colder climate areas

Water Pipe Types – 2 of 2

- **Pre-action System**
  - Combo of wet and dry pipe system
  - Water released into pipe and link must melt before water is released
  - Better support for false alarms or another method of putting fire out

- **Deluge System**
  - Same as dry pipe but the sprinkler head is open
  - Releases a lot of water fast
  - Not appropriate for a data processing environment
- **Both require a supplemental system of detection**

Dry Pipe System



Fire Extinguishers

- Within 50 feet of electrical equipment
- Inspected quarterly
- Clearly marked with unobstructed view
- Easily reached
- Filled with appropriate and approved suppression agent

Agenda

- Understand site and facility design considerations
- Support the implementation and operation of perimeter security (e.g., physical access control and monitoring, audit trails/access logs)
- Support the implementation and operation of internal security (e.g., escort requirements/visitor control, keys and locks)
- Support the implementation and operation of facilities security (e.g., technology convergence)
- Support the protection and securing of equipment
- **Understand personnel privacy, safety and threats (e.g., duress, travel, monitoring)**

Administrative Controls

- **Management Responsibilities**
  - Emergency response and procedures
  - Periodic inspections and reports
  - Awareness and training
  - Drills and exercises
    - Simulation testing
  - Facility management
  - Personnel control

- **Threats**
  - Usually uncovered during disaster recovery analysis
  - Many of these issues are rolled into disaster recovery and business continuity

Threat – Piggybacking/ Tailgating

- Piggybacking or tailgating, is when an individual gains unauthorized access by using someone else's legitimate credentials or access rights

- Usually an individual just follows another person closely through a door without providing any credentials

- The best preventive measure against this type of a problem is a security guard and employee education on good security practices

- Mantraps are effective controls against piggybacking

Threats to Device Security

- **Portable Devices (Laptops, USB Drives, PDA, SD Cards, etc.)**
  - Locking mechanism
  - Tracing software
  - Encryption
  - Inventory system
  - Anti-virus software

- **Critical or sensitive items should be placed in security containers**
  - Safes, vaults, locking file cabinets
  - Should be fire and theft resistant

- **Good lock combinations that are changed frequently and distribution monitored**

Threats to Physical Security

- Physical damage (both infrastructure and hardware)
- Theft
- Interruption of services (power failure)
- Unauthorized disclosure of information
- Natural disasters
- Fires
- Vandalism
- Terrorism
- Environmental issues

Vulnerability Assessment

- Inspections
- Facility location and construction
- Training
- Review history of losses
- Current controls