CISSP® Common Body of Knowledge Review:

Physical (Environmental) Security Domain

Version: 5.10

Learning Objective

Physical (Environmental) Security Domain

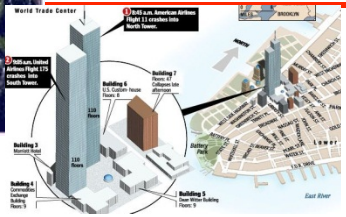
The Physical (Environmental) Security domain addresses the threats, vulnerabilities, and countermeasures that can be utilized to physical protect an enterprise's resources and sensitive information. These resources include people, the facility in which they work, and the data, equipment, support systems, media, and supplies they utilize.

Physical security describes measures that are designed to deny access to unauthorized personnel (including attackers) from physically accessing a building, facility, resources, or stored information; and guidance on how to design structures to resist potentially hostile acts.

The candidate is expected to know the elements involved in choosing a secure site, its design and configuration, and the methods for securing the facility against unauthorized access, theft of equipment and information, and the environmental and safety measures needed to protect people, the facility, and its resources.

Reference: *CISSP CIB*, January 2012 (4.17.14 Rev. 13)

Lessons-Learned for U.S.



- Major Domestic Events:
  - 2005 Hurricane Katrina (1,836)
  - 2001 9/11 Attack: World Trade Center, Pentagon, and Shanksville, PA (2,982)
  - 1995 Federal Office Building, Oklahoma City (168)

- Major International Events:
  - 1998 U.S. Embassy, Kenya (237)
  - 1983 Beirut Barracks, Lebanon (309)

An aerial view of the American Embassy as heavy cranes continue to remove rubble from the upper floors on 21 April, 1983, following the terrorist bombing three days earlier.

Photo courtesy of Claude Salhani / U.S. Marines in Lebanon 1982-1984 History and Museums Division, Headquarters, U.S.M.C., Washington, D.C.

Reference:
List of Terrorist Attacks, Wikipedia (http://en.wikipedia.org/wiki/List_of_battles_and_other_violent_events_by_death_toll#Terrorist_attacks)

References for Physical Security

- Interagency Security Committee (ISC)
  - Facility Security Level Determinations for Federal Facilities (21 February 2008)
  - Physical Security Criteria for Federal Facilities (12 April 2010)
  - Design-Basis Threat (12 April 2010)
  - The Use of Physical Security Performance Measures (June 2009)
- Department of Defense (DoD)
  - Unified Facility Criteria (UFC) 4-010-01, Minimum Antiterrorism Standards for Buildings (22 January 2007)
  - UFC 4-020-01, DoD Security Engineering Facility Planning Manual
- Department of State (DoS)
  - OBO-ICS 2009, Overseas Building Operations International Code Supplement
- Commercial Facilities
  - Crime Prevention Through Environmental Design (CPTED)
  - Structural Design for Physical Security, State of the Practice, Structural Engineering Institute, American Society of Civil Engineers (ASCE)

Reference:
Security for Building Occupants and Assets, National Institute of Building Science (http://www.wbdg.org/design/provide_security.php)

Topics

Physical Security Domain

- ➡ Terms & Definition
- Type of Threats and Information Protection Environment
- Security Countermeasures & Technologies

Categories of Security Controls

- Management (Administrative) Controls
  - Policies, Standards, Processes, Procedures, & Guidelines
    - Administrative Entities: Executive-Level, Mid.-Level Management
- Physical Controls
  - Physical Security (Facility or Infrastructure Protection)
    - Locks, Doors, Walls, Fence, Curtain, etc.
    - Service Providers: FSO, Security Guards, Dogs
- Technical (Logical) Controls
  - Access Controls , Identification & Authorization, Confidentiality, Integrity, Availability, Non-Repudiation.
    - CCTV & Camera, IDS, Moisture detection system, Fire/Smoke detection system, Fire suppression, Environmental control system, UPS, etc.
    - Service Providers: Building Architect, Critical Infrastructure Protection (CIP) Engineer, Operations Center.

Types of Security Controls

- Directive controls: Often called administrative controls, these are intended to advise employees of the behavior expected of them during their interfaces with or use the organization's information systems.
- Preventive controls: Included in preventive controls are physical, administrative, and technical measures intended to preclude actions violating policy or increasing risk to system resources.
- Deterrent controls: Deterrent controls involve the use of warnings of consequences to security violations.
- Detective controls: Detective controls involve the use of practices, processes, and tools that identify and possibly react to security violations.
- Corrective controls: Corrective controls also involve physical, administrative, and technical measures designed to react to detection of an incident in order to reduce or eliminate the opportunity for the unwanted event to recur.
- Recovery controls: Once an incident occurs that results in the compromise of integrity or availability, the implementation of recovery controls is necessary to restore the system or operation to a normal operating state.

Topics

Physical Security Domain

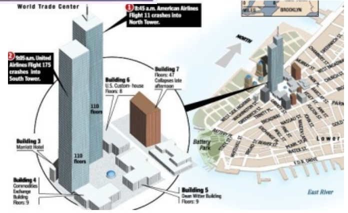
- Terms & Definition
- Type of Threats and Information Protection Environment
- Security Countermeasures & Technologies

Type of Threats to Physical Environment

- Natural / Environmental
  - Earthquakes, floods, storms, hurricanes, fires, snow/ice
  - Consequence of natural phenomena
- Man made / Political Events
  - Explosives, disgruntled employees, unauthorized access, employee errors, espionage, arson/fires, sabotage, hazardous/toxic spills, chemical contamination, malicious code, vandalism and theft
  - Acts of commission or omission

Lessons-Learned for U.S.

- Major Domestic Events:
  - 2005 Hurricane Katrina (1,836)
  - 2001 9/11 Attack: World Trade Center, Pentagon, and Shanksville, PA (2,982)
  - 1995 Federal Office Building, Oklahoma City (168)



- Major International Events:
  - 1998 U.S. Embassy, Kenya (237)
  - 1983 Beirut Barracks, Lebanon (309)

An aerial view of the American Embassy as heavy cranes continue to remove rubble from the upper floors on 21 April, 1983, following the terrorist bombing three days earlier.

Photo courtesy of Claude Salhani / U.S. Marines to Lebanon 1982-1984 History and Museums Division, Headquarters, U.S.M.C., Washington, D.C.

Reference:
List of Terrorist Attacks, Wikipedia (http://en.wikipedia.org/wiki/List_of_battles_and_other_violent_events_by_death_toll#Terrorist_attacks)

Example References for Physical Security

- Interagency Security Committee (ISC)
  - *Facility Security Level Determinations for Federal Facilities* (21 February 2008)
  - *Physical Security Criteria for Federal Facilities* (12 April 2010)
  - *Design-Basis Threat* (12 April 2010)
  - *The Use of Physical Security Performance Measures* (June 2009)
- Department of Defense (DoD)
  - Unified Facility Criteria (UFC) 4-010-01, *Minimum Antiterrorism Standards for Buildings* (22 January 2007)
  - UFC 4-020-01, *DoD Security Engineering Facility Planning Manual*
- Department of State (DoS)
  - OBO-ICS 2009, *Overseas Building Operations International Code Supplement*
- Commercial Facilities
  - Crime Prevention Through Environmental Design (CPTED)
  - *Structural Design for Physical Security, State of the Practice*, Structural Engineering Institute, American Society of Civil Engineers (ASCE)
  - And many others…

Reference:
Security for Building Occupants and Assets, National Institute of Building Science
(http://www.wbdg.org/design/provide_security.php)

Security Objectives & Controls

Safeguarding and protecting physical assets against damage, lost, or theft from natural/environmental and man-made/political events.

- Administrative controls
  - Facility location, construction, and management.
  - Physical security risks, threats, and countermeasures.
- Technical controls
  - Authenticating individuals and intrusion detection.
  - Electrical issues and countermeasures.
  - Fire prevention, detection, and suppression.
- Physical controls
  - Perimeter & Building Grounds.
  - Building Entry Point.
  - Box-within a box Floor Plan.
  - Data Centers or Server Room Security.

Topics

Physical Security Domain

- Terms & Definition
- Type of Threats and Information Protection Environment
- ➡ Security Countermeasures & Technologies

Strategic Approach to Physical Security ...(1/2)

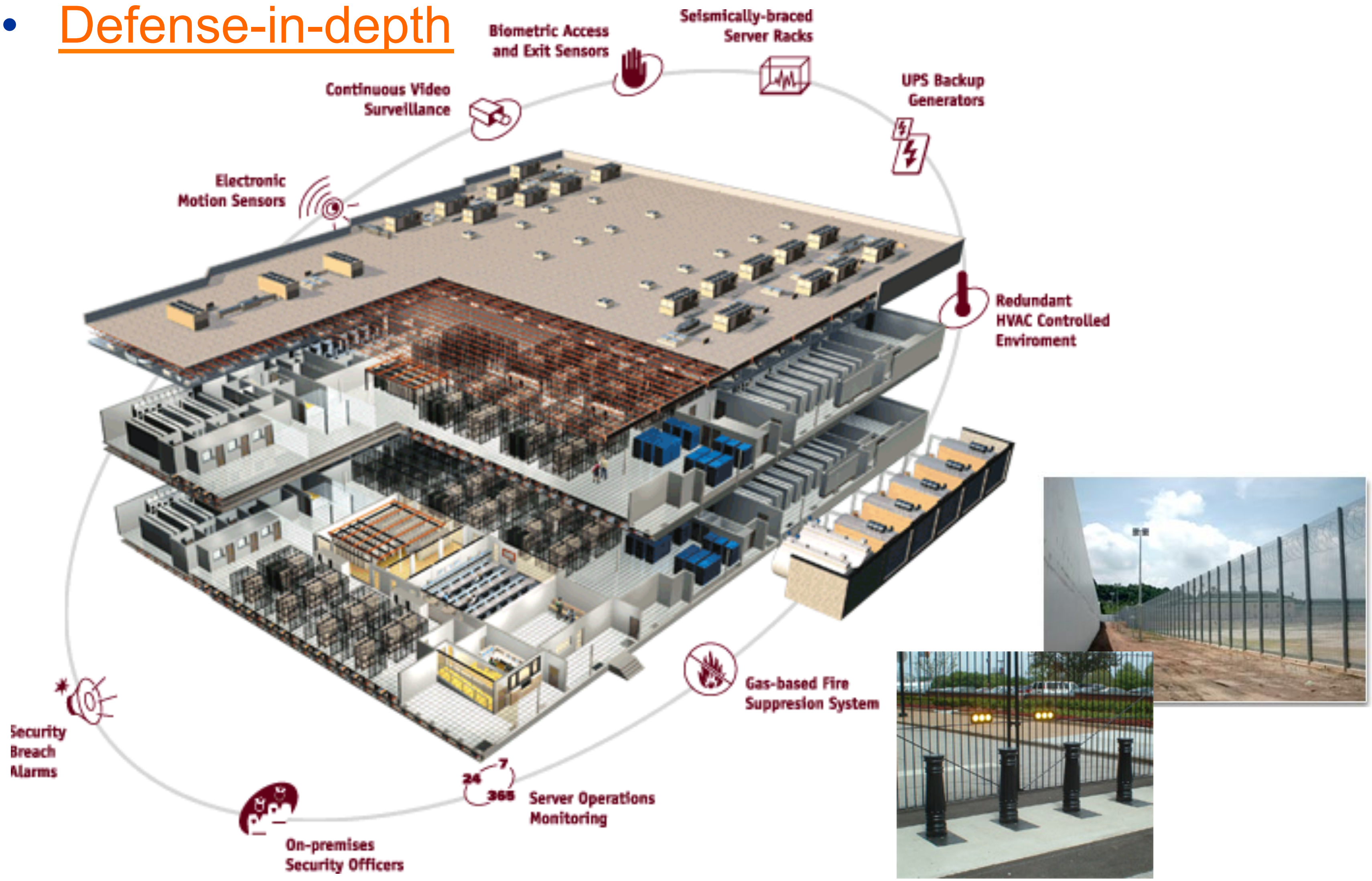
- Facility location, construction, and management using Crime Prevention through Environmental Design (CPTED)
  - Natural Surveillance
    - Architectural features that maximizes visibility of people, parking areas, and building entrances.
  - Territorial Reinforcement
    - Architectural features that distinguishes private and public spaces (e.g., fences, gateways, and landscape, etc.)
  - Natural Access Control
    - Structural elements that discourages access to private areas (e.g., streets, signs, and landscape, etc.)
  - Target Hardening
    - Architectural elements that prohibits unauthorized accesses (e.g., door locks, window locks, interior door hinges, etc.)

Reference: http://cpted-watch.com

Security Countermeasures & Technologies

Strategic Approach to Physical Security …(2/2)

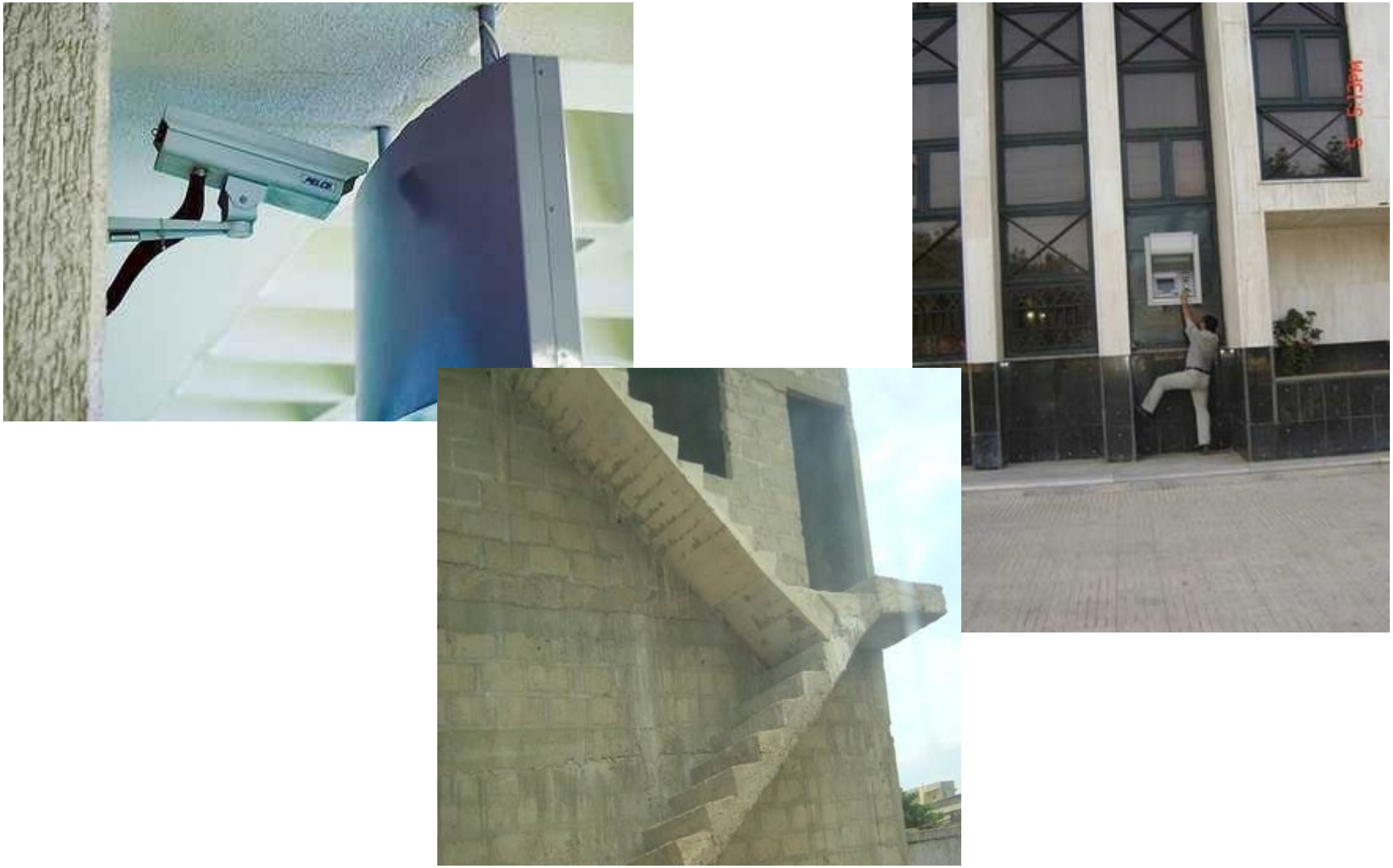
- Defense-in-depth


Biometric Access and Exit Sensors
Seismically-braced Server Racks
Continuous Video Surveillance
UPS Backup Generators
Electronic Motion Sensors
Redundant HVAC Controlled Enviroment
Gas-based Fire Suppresion System
Security Breach Alarms
24 7 365 Server Operations Monitoring
On-premises Security Officers

Source: Global Crossing website

Reference:
Verizon-Terremark (http://www.datacenterknowledge.com/archives/2011/04/11/verizon-completes-acquisition-of-terremark/)

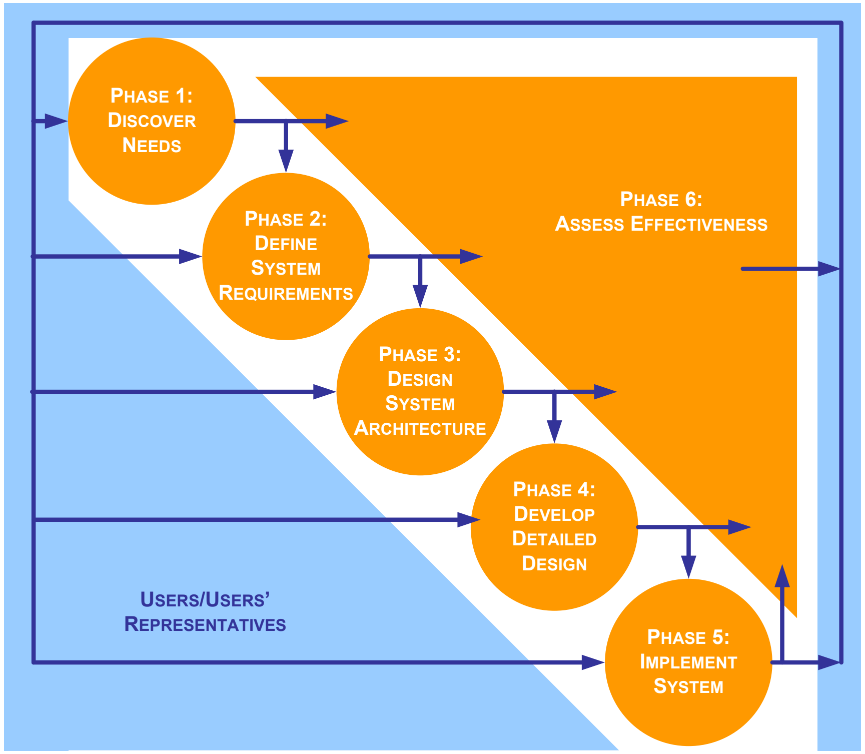
Examples of Design Failure



More Examples of Design Failure

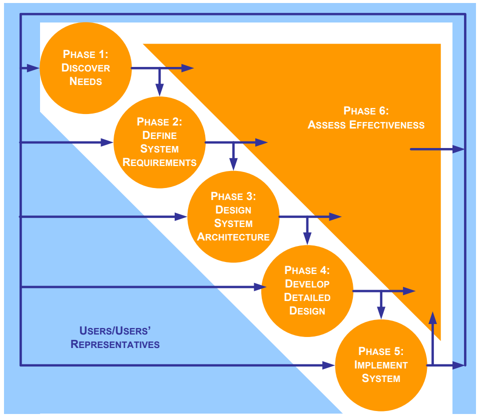
Design Process

- Similar to information system, physical security system also uses SDLC process…
- Development of physical security system starts with Business /Mission needs.



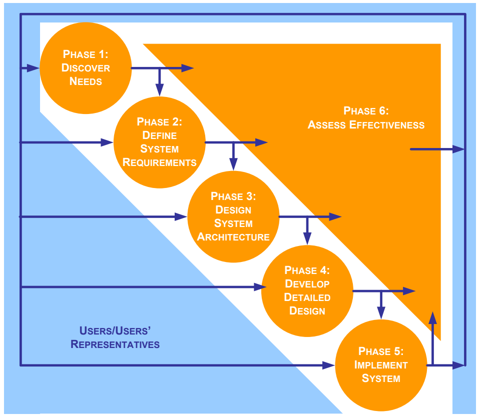
Defining Business/Mission Needs

- Security considerations for building location and how it should be built.
  - Natural disasters?
  - Adjacent buildings?
  - Crime?
  - Riots?
  - Airport?
  - Highway?
  - Power source?
  - Water source?
  - Emergency support?
  - Fire station?
  - Hospital?



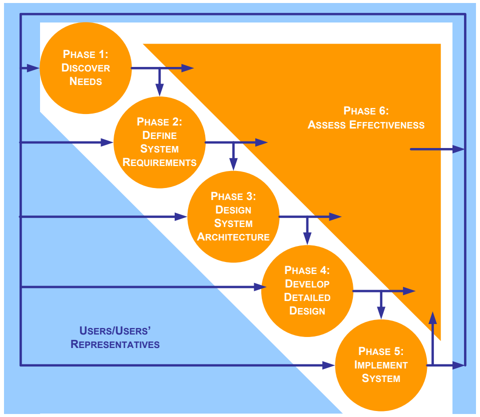
Plan and Define Physical Security Requirements

- Perform critical-path analysis for site location, construction impacts, and facility impacts.
  - Lists all elements of physical security and how they interact and how they are interdependent.
    - (i.e. power, data, water, A/C, generators, storm drains, and sewer lines).
  - Path that is critical for business functionality.
  - Alignment to business continuity, COOP, and disaster recovery goals.
    - Business impact analysis (BIA).
    - Information sensitivity or classification.
  - Consider laws and regulations. (e.g. building codes, fire codes, etc.)


Phase 1: Discover Needs
Phase 2: Define System Requirements
Phase 3: Design System Architecture
Phase 4: Develop Detailed Design
Phase 5: Implement System
Phase 6: Assess Effectiveness
Users/Users' Representatives

Facility – Location

- Location Considerations
  - Natural disasters (i.e. floods, tornadoes, earthquakes, or hurricanes.)
  - Hazardous terrain (i.e. mudslide, excessive snow or rainfall.)
  - Surrounding area and external entities
    - Local crime rate / Riots.
    - Proximity to police, medical, and fire stations.
    - Potential hazards from surrounding area.
  - Accessibility
    - Road access.
    - Excessive traffic.
    - Proximity to airports, train stations, and highways.
  - Visibility
    - Building markings and signs.
    - High or low population in the area.
    - Types of neighbors.

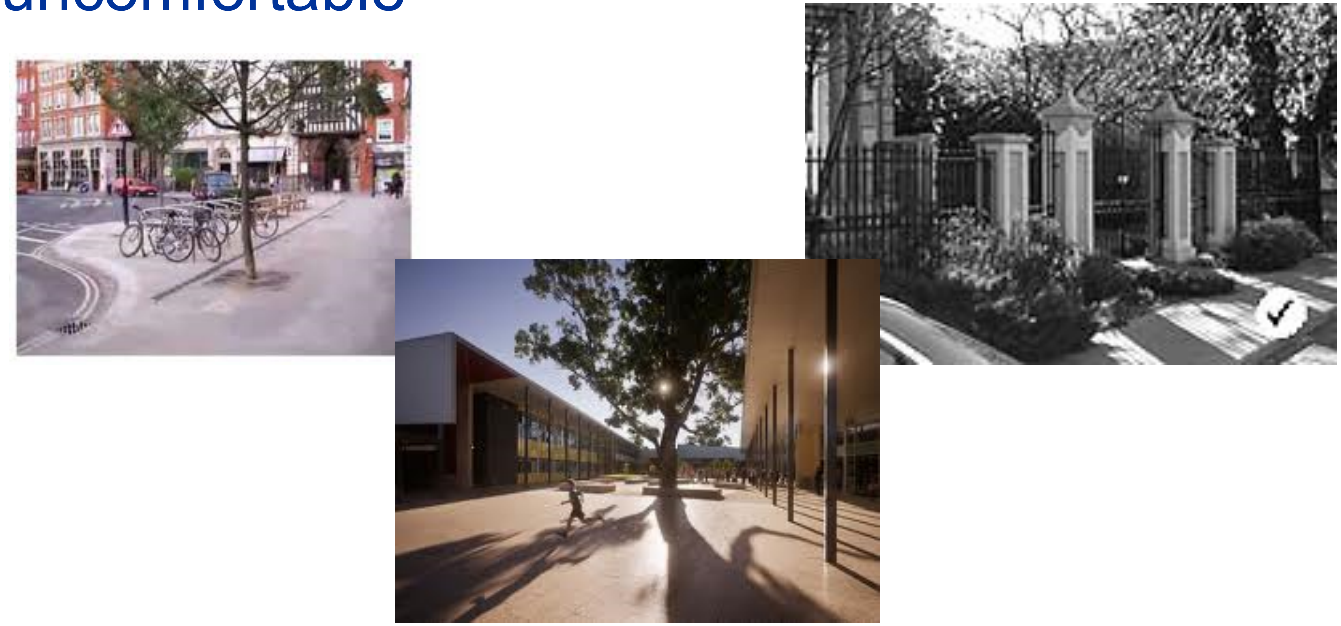

Phase 1: Discover Needs
Phase 2: Define System Requirements
Phase 3: Design System Architecture
Phase 4: Develop Detailed Design
Phase 5: Implement System
Phase 6: Assess Effectiveness
Users/Users' Representatives

CPTED – Natural Access Control

- Terrain
  - Distance from fenced boundary to building. Distance to adjacent building or structure.
  - Roadway and paths to building(s).
- Landscaping
  - Spiny shrubs and/or trees
  - Grass, sod or gravel traps
  - Water (i.e. drainage pond, lake or stream)

CPTED – Natural Surveillance

- Use and placement of physical environmental features, personnel walkways, and activity areas in ways that maximize visibility
- Open stairways
- Make employees feel safe and intruders feel uncomfortable

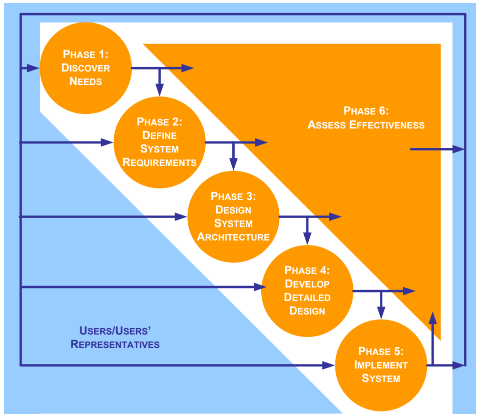


CPTED – Territorial Reinforcement

- Physical designs that emphasize or extend the company’s physical sphere of influence so that legitimate users feel a sense of ownership of that space
- Use walls, fences, flags, etc.
- Create a sense of dedicated community

CPTED – Target Hardening

- Building access controls
  - Entry/ exit points
  - Windows and doors
  - Interior partitions (e.g., walls, ceilings, and floors, etc.)
  - Locks
  - Intrusion detection
- Utilities
  - Power sources: primary and backup
  - Water sources and sewage
- Air conditioning
  - Heating & cooling
  - Humidity control
- Fire controls
  - Detection and mitigation


Phase 1: Discover Needs
Phase 2: Define System Requirements
Phase 3: Design System Architecture
Phase 4: Develop Detailed Design
Phase 5: Implement System
Phase 6: Assess Effectiveness
Users/Users' Representatives

Administrative Controls

- Physical security policies & procedures
  - Response measures and procedures
    - Integration with business continuity, COOP, and disaster recovery plans.
    - Periodic inspections and reports.
    - Awareness training, testing and drills.
  - Risk Management processes
    - Risk assessment to identify threats and threat agents
    - Risk mitigation to plan for change and update baseline
    - Risk evaluation to verify & validate countermeasures.
  - Security audits & assessments
    - Review audit trails of entries and exits.
    - Perform assessments using walkthrough (desktop exercise), checklist, simulation, or full-interrupt test.

Administrative Controls

- Security guards are used for making complex decisions:
  - Checking credentials at entry points.
  - Ensuring company property does not leave facility.
  - Monitor intrusion detection and fire alarm systems.
  - Verify doors and windows are locked.
  - Watching for suspicious activity.
  - Watch for piggybacking.
  - Should not stay stationary – may have a post and one roving guard.
  - Personnel is the most expensive countermeasure to reduce physical security risks.

Physical Controls – Facility Construction

- Structured barriers: Perimeter structure
- Walls & Fencing
  - Specific gauge and fabrication specifications (e.g. No. 11 gauge galvanized chain-link fencing material.)
  - Specify height, or need for "top guard" (e.g. 8-ft in height, 6-in. under ground with top guard.)

Height	Protection
1 meter / 3 – 4 ft	Deters casual trespassers
2 meter / 6 – 7 ft	Too high to climb easily
2.4 meter / 8 ft with top guard	Deters determined intruder

Source: *Official (ISC)^2 Guide to The CISSP Exam*

Physical Controls – Facility Construction

- Structured barriers: Entry points
  - Gates, bollards, roadways.
  - Doors, windows, ventilation airways, manhole covers, etc.
  - Department of State and DoD Anti-Ram Vehicle Barrier Certification Criteria (SD-STD-02.01):

Vehicle Weight: 15,000 lb.	
Speed Rating	**Speed at Impact**
K4	30 mph
K8	40 mph
K12	50 mph

Vehicle Weight: 15,000 lb.	
Penetration Rating	**Penetration Distance**
L3	< 3 ft
L2	3 – 20 ft
L1	20 – 50 ft

VehicleBarrier.wmv

Reference: http://www.probarrier.com/faq/certify.asp

Physical Controls – Facility Construction

- Structured barriers: Standard for vehicular gates (UL Standard 325)
  - **Class I:** Residential gate operation
  - **Class II:** Commercial, such as a parking lot or garage
  - **Class III:** Industrial/ limited access, such as a warehouse, factory, or loading doc
  - **Class IV:** Restricted access operation that requires supervision by security personnel, such as those at a prison or airport security area

Reference: *Official (ISC)2 Guide to The CISSP Exam*

Physical Controls – Facility Construction

- Structured barriers: Construction materials
  - Exterior / interior walls (i.e. structural, sound, and TEMPEST.)
  - Windows (e.g. structural, exposure to sun light, size & height.)
  - Ceiling, roof, and floor (e.g. structural, and access.)
  - Structural (i.e. earthquake proofing, and fire resistance.)

Reference: *Official (ISC)2 Guide to The CISSP Exam*

Physical Controls

- Lighting
  - Provide deterrent to intruders and to assist other access control systems.
  - Types of lighting systems:
    - Continuous lighting: A series of fixed luminaries arranged to flood a given area continuously
    - Trip lighting: Activated when intruder crosses a sensor
    - Standby lighting: Similar to continuous lighting, except luminaries are not continuously lit
    - Emergency lighting: Activated in emergency events (e.g. power failure or fire)
  - Types of lighting:
    - Glare projection lighting: To a specific area and deter intruder actions
    - Flood light: To a large area to facilitate security monitoring

Reference: *Official (ISC)2 Guide to The CISSP Exam*

Questions:

- What is the primary rationale for having a security guard?
  –

- What are the three types of structured barrier that provide physical protection of assets within a facility?
  –
  –
  –

- What are the two type of natural barrier that provide physical protection of assets within a facility?
  –
  –

Answers:

- What is the primary rationale for having a security guard?
  - To make complex decision
- What are the three types of structured barrier that provide physical protection of assets within a facility?
  - Perimeter structures
  - Entry point controls
  - Construction material
- What are the two type of natural barrier that provide physical protection of assets within a facility?
  - Terrain
  - Landscaping

Questions:

- What is the minimum fencing requirement for deterring a determined intruder?
  -
- What is the minimum entry point barrier standard that would stop a 15k lb (or 7 ton) truck at 30 mph?
  -
- What are the two primary purposes for lighting?
  -
  -

Answers:

- What is the minimum fencing requirement for deterring a determined intruder?
  - 8 ft with top guard

- What is the minimum entry point barrier standard that would stop a 15k lb (or 7 ton) truck at 30 mph?
  - K4 (for 30 mph), K8 (for 40 mph), K12 (for 50 mph)

- What are the two primary purposes for lighting?
  - Deter intruders
  - Assist in identification of intruders

Technical Controls – Entrance Protection

Entry access control systems

- Turnstiles
  - Revolving doors that can be activated to "lock" and not allow unauthorized individuals to enter or leave facility
  - To prevent "piggybacking".
- Mantraps
  - Routing people through two stationary doorways
- Fail-safe
  - Door defaults to being unlocked.
- Fail-secure
  - Door defaults to being locked.

Technical Controls

Entry access control systems – Locks

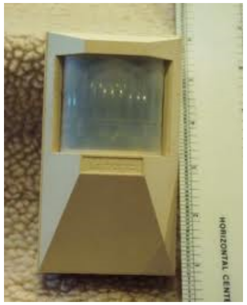
- Mechanical locks:
  - Key
  - Combination locks
  - Magnetic locks

- Electronic locks:
  - Combination lock
  - Proximity / RFID badge
  - Bio-metric

Technical Controls

Intrusion detection & surveillance systems

- IDS: Sensors that detect access into a controlled area:
  - Photoelectric
  - Ultrasonic
  - Microwave
  - Passive infrared
  - Pressure sensitive



Technical Controls – Intrusion Detection & Surveillance Systems

- Closed-circuit television (CCTV)
  - Detect the presence of an object.
  - Recognition of object type.
  - Identification of object details.

Technical Controls – Surveillance Systems

- CCTV camera considerations
  - Charge-coupled device (CCD) converts pixels into data signals
  - Cathode ray tube (CRT) converts picture image into data signals
  - Field-of-view is the area that can be captured by the camera lens.
  - Depth-of-field is the area between the nearest and farthest points that appear to be in focus.
  - Monochrome or color camera.

Technical Controls – Electrical Power Supply

- Risks to electrical power supply:
  - Blackout: complete loss of commercial power
  - Fault: momentary power outage
  - Brownout: an intentional reduction of voltage by a power company.
  - Sag/dip: a short period of low voltage
  - Surge: a sudden rise in voltage in the power supply.
  - In-rush current: the initial surge of current required by a load before it reaches normal operation.
  - Transient: line noise or disturbance is superimposed on the supply circuit and can cause fluctuations in electrical power

Technical Controls – Electrical Power Supply

- Counter measures to electrical power supply risks:
  - Uninterruptible power supply (UPS) (include transfer switch, battery, transformer, generator, circuit switch, and power distribution unit (PDU))
    - For blackout and fault
  - Surge protector, circuit breaker, transformer, and UPS
    - For brownout, sag/dip, surge, in-rush current, and transient

From Computer Desktop Encyclopedia
Reproduced with permission.
© 2009 American Power Conversion Corp.

Technical Controls – Electrostatic Discharge

- Risk of electrostatic discharge:
  - A type of electrical surge can occur when two non-conducting materials rub together, causing electrons to transfer from one material to another.
- Countermeasures: Anti-electrostatic discharge (ESD) standards
  - Grounding of equipment to a common point ground.
  - Grounding of personnel: wrist strap, flooring, clothing and footwear.
  - Protected area: Flooring, seating, ionization of air, and humidity control.
  - Marking of equipment, package and facility.
  - Example: Data center: grounding of rack & floors to a common point ground, raised floor tiles have conductive gold leafs to supporting frame to dissipate ESD.

Technical Controls – Heating, Ventilating and Air Conditioning (HVAC)

- Types of HVAC systems:
  - Up-flow (forced air above the floor) vs. down-flow (forced air below the raised floor).
  - Water or Glycol.

- HVAC considerations:
  - Air volume cubic feet per minute (CFM) per ton.
  - Humidity control (RH 45% - 60%).
  - Temperature control (72°F ± 2°F).
  - Air Filters.
  - Positive air pressure.
  - Protected intake vents.
  - Alarms: Leak detection, loss of power, temperature, humidity, fire, smoke detector.

Technical Controls – Water Supply System

- For cooling, plumbing, sewage, and fire-suppression (outside of server room).
- Water source.
- Water usage.
  - Volume of water.
  - Water filtration.
  - Environmental impact.
- Water pump to maintain pressure.

Technical Controls – Types of Fire

Fire Class	Type of Fire	Elements of Fire	Suppression Method
Class A	Common Combustibles	Ashes, paper, wood, cloth, etc.	Water, Soda acid
Class B	Liquid	Barrels of oils, Petroleum, tars, solvents, alcohol, gases	Halon, CO_2, FM-200
Class C	Electrical	Circuits, electrical equipment, and wires	Halon, CO_2 , or Non-conductive extinguishing agent – FM-200
Class D	Dry Chemical	Combustible metals, and chemical	Dry Powder, Halon
Class K	Commercial Kitchen	Food, Grease	Wet Chemicals - Foam

Technical Controls – Fire Suppression Systems

- Halon
  - Used so that equipment is not damaged by water.
- FM-200
  - Replacement for Halon without ozone depleting chemicals.
  - It uses chemicals instead of water.

- Carbon Dioxide
  - Does not leave reside after use, does not cause damage to sensitive devices.
  - Can suffocate people.

- Dry Chemicals
  - Not effective against electrical fires.

Technical Controls – Fire Suppression Systems

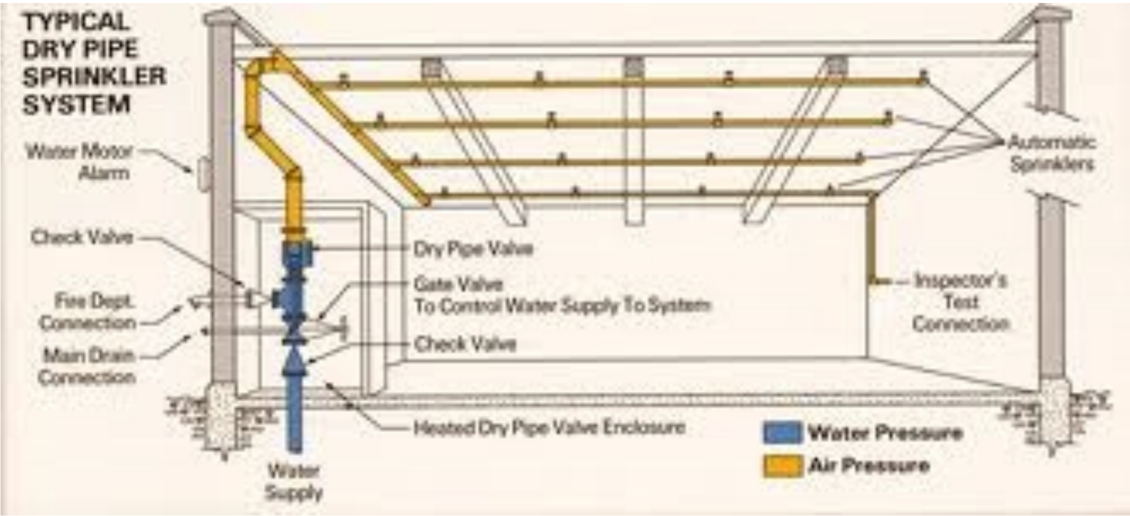
Special note on fire suppression systems…

- Halon
  - Halon has been banned for all new fire suppression systems under the 1987 Montreal Protocol on Substances that Deplete the Ozone Layer.
    - Began implementation in 1992. All new installations of fire suppression systems must use alternate options.
- "Pre-action" or dry-pipe fire suppression system
  - Water is held back remotely by a valve that is actuated by a sensing system.
- Deluge fire suppression system
  - Same as dry pipe except the sprinkler head is open.
  - Releases a lot of water fast.
  - Usually not used in data processing environments.

Temperature	Color
155° F	Red
174° F	Yellow
200° F	Green

Technical Controls – Fire Suppression Systems

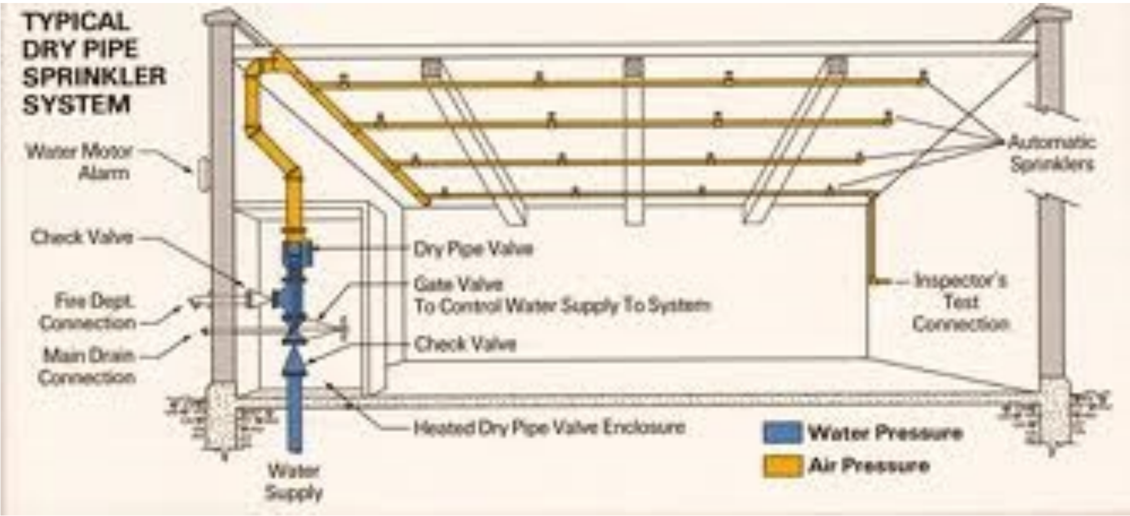
- Dry Pipe:
  - No water standing in the pipe
  - Air is blown out and water is released
  - Time delay can allow systems to properly power down



Reference: *Fundamentals of Fire Fighter Skills*, International Association of Fire Chiefs, 2008

Technical Controls – Fire Suppression Systems

- Pre-action:
  - Form of dry pipe system
  - Has a secondary device such as smoke detector or manual-pull alarm
  - Requires activation of the secondary device before water is released



Reference: *Fundamentals of Fire Fighter Skills*, International Association of Fire Chiefs, 2008

Technical Controls – Fire/ Smoke Detection

- Ionization-type smoke detector detect charged particles in smoke.

- Optical (photoelectric) smoke detectors react to light blockage because of smoke.

- Fixed or rate-of-rise temperature sensor.

Questions:

- Turnstiles access control system prevents?
  -
- What is the difference between fail-safe door and a fail-secure door?
  -
  -
- What are the two types of error rate for bio-metric access control systems?
  -
  -

Answers:

- Turnstiles access control system prevents?
  - “Piggybacking”

- What is the difference between fail-safe door and a fail-secure door?
  - Fail-safe defaults to being unlocked
  - Fail-secure defaults to being locked

- What are the two types of error rate for bio-metric access control systems?
  - False rejection (Type I Error)
  - False acceptance (Type II Error)

Questions:

- What is the term for describing a complete loss of commercial power?
  -

- What is the term for describing a sudden rise of voltage in the power supply?
  -

- What is the term for describing a momentary power outage?
  -

Answers:

- What is the term for describing a complete loss of commercial power?
  - Blackout

- What is the term for describing a sudden rise of voltage in the power supply?
  - Surge

- What is the term for describing a momentary power outage?
  - Fault

Questions:

- How humidity control can reduce the risk of electrostatic discharge?
  - –

- What class of fire is caused by electrical elements?
  - –

- Why type of fire suppression system were the water is held back remotely by an actuator?
  - –

- What type of fire suppression system releases a lot of water fast?
  - –

Answers:

- How humidity control can reduce the risk of electrostatic discharge?
  - By reduce ionization of air particles

- What class of fire is caused by electrical elements?
  - Class C

- Why type of fire suppression system were the water is held back remotely by an actuator?
  - Dry-pipe (a.k.a. pre-action)

- What type of fire suppression system releases a lot of water fast?
  - Deluge

Validation Time… ☺

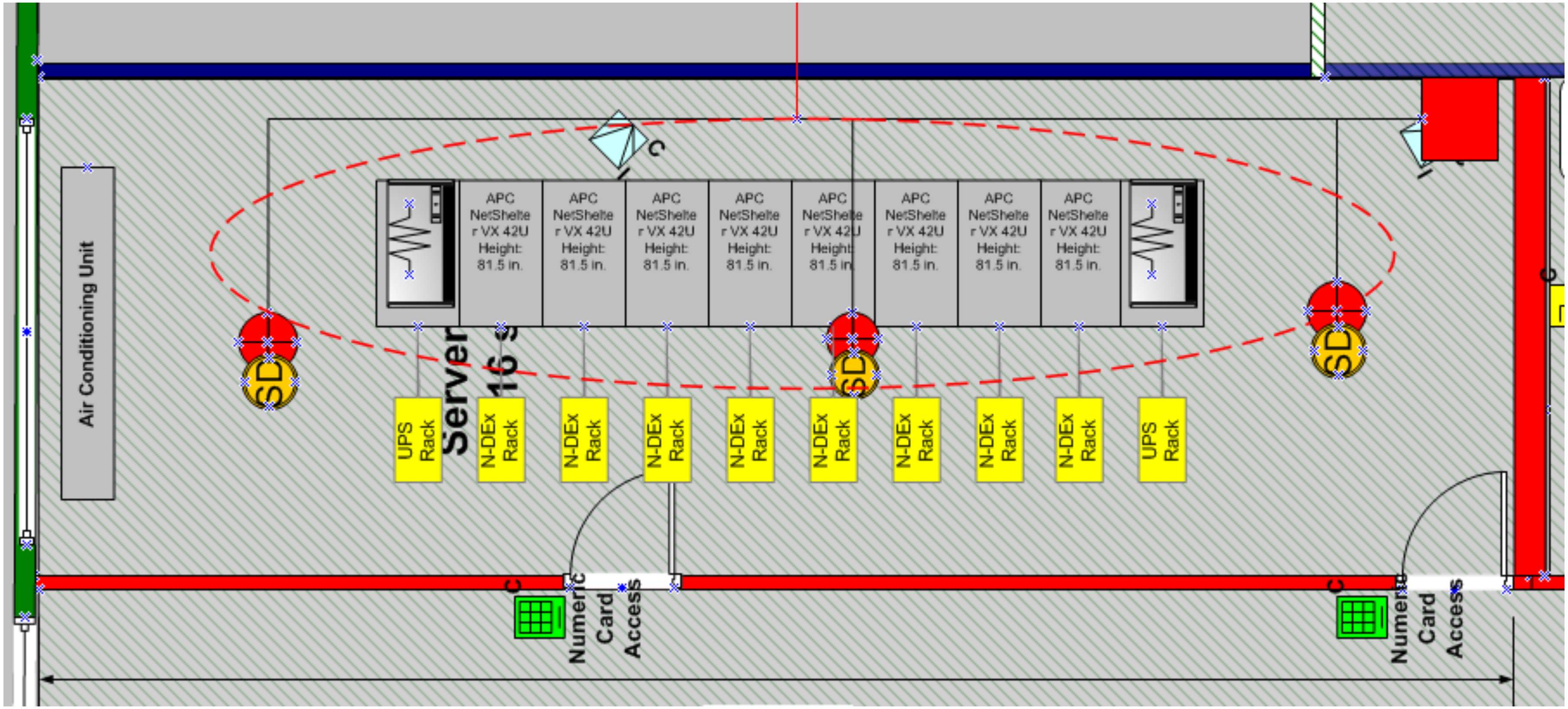
1. Classroom Exercise

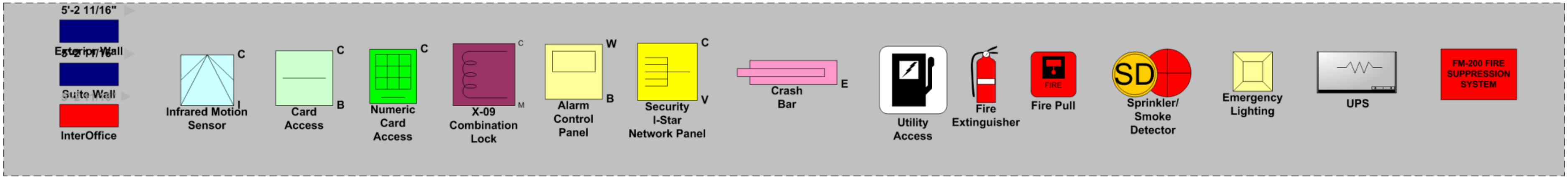
2. Review Answers

Exercise #1: Electrical Utility Definition

Electrical Power Terminology	Description
Fault	
Blackout	
Sag/Dip	
Brownout	
Spike	
Surge	
Inrush Current	
Noise	
Transient Noise	
Clean	
Ground	

Exercise #2: What do you think it might be missing?





LEGEND

Suggested

ANSWERS

Exercise #1: Electrical Utility Definition

Electrical Power Terminology	Description
Fault	Momentary loss of power
Blackout	Complete loss of power
Sag/Dip	Momentary low voltage
Brownout	Prolonged low voltage
Spike	Momentary high voltage
Surge	Prolonged high voltage
Inrush Current	Initial surge of power
Noise	Steady interference
Transient Noise	Short duration of line noise
Clean	Non-fluctuating power
Ground	One wire is grounded

Exercise #2: What do you think it might be missing?