CISSP Physical Security

- Administrative Personnel Controls
  - Normally implemented by HR
  - Pre-employment screening
    - References
    - Background checks
    - Security clearances
  - On-going employee checks
    - Reviews
    - Exit interview
  - Post-employment
    - Removal of network access
    - Return of equipment
- Environmental and Life Safety
  - Noise and Power
    - Noise
      - EMI
        - Common Mode
          - Presence of electrical radiation in the system
          - Interferes with Clean power
        - Traverse Mode
          - Live and earth
          - Live and neutral
      - RFI
    - Protective measures
      - Power Line Conditioning
      - Proper Earthing
      - Cable shielding
      - Limit exposure to magnets, fluorescent lights, motors, and space heaters
    - Subtopic
  - Electrical Power
    - Brownouts
      - ANSI
        - Allow 8% drop between building meter and power source
        - Allow 3.5% drop from meter to the wall
    - Humidity
      - Ideal 40% to 60%
        - Below 40%
          - Causes Static
        - Above 60%
          - Results in corrosion
      - Static Charges Will damage
        - 40V
          - Sensitive Circuits
        - 1000V
          - Monitor displays scramble
        - 1500V
          - HDD data loss
        - 2000V
          - System shutdown
        - 4000V
          - Printer jam
        - 17000V
          - Chip damage
      - Prevent Static
        - Anti-static sprays
        - Proper Earthing
        - Anti-static cables
        - Anti-static flooring
        - HVAC to maintain humidity
    - Fault conditions
      - Fault
        - Momentary loss of power
      - Blackout
        - Complete loss of power
      - Sag
        - Momentary low voltage
      - Brownout
        - Prolonged low voltage
      - Spike
        - Momentary high voltage
      - Surge
        - Prolonged high voltage
      - Inrush
        - Initial surge of power
      - Noise
        - Steady interference
      - Transient
        - Short duration of line noise
      - Clean
        - Non fluctuating power
      - Ground
        - One wire is grounded
  - Fire detection and suppression
    - Three elements to sustain fire
      - Oxygen
      - Heat
      - Fuel
    - Classes
      - Class A
        - Common Combustibles
          - Water or Soda Acid
      - Class B
        - Liquid
          - CO2, Soda Acid, Halon
      - Class C
        - Electrical
          - CO2 or Halon
      - Class D
        - Combustible Metals
          - Dry Powder
    - Defeating
      - Water
        - Lowers temp
      - Soda Acid
        - Starves of Oxygen
      - CO2
        - Removes Oxygen
      - Halon
        - Creates a chemical reaction that kills the fire
    - Fire Detectors
      - Heat Sensing
      - Flame Actuated
      - Smoke Actuated
    - Sprinklers
      - Wet pipe
        - Fusible link goes at 165F
      - Dry Pipe
        - Can give time delay as air is blown out first
      - Deluge
        - Large volume of water
      - Preaction
        - Common in Computer Rooms
        - Charges pipe when heat is detected
        - Fusible link melts when hot enough
    - Halon
      - 1211
        - PFE
          - Liquid streaming
        - being replaced
      - 1301
        - Installations
        - No new ones allowed
        - being banked
      - Substitutes
        - Fm-200
          - Most common
        - Argon
        - Inergen
    - Temp Damage Points
      - Computer Hardware
        - 175F
      - Magnetic Storage
        - 100F
      - Paper
        - 350F
- Heating Ventilation and Air Conditioning (HVAC)

Administrative Personnel Controls

Physical and Technical Controls

- Physical Technical Controls
  - Guards
  - Dogs
  - Fencing
    - 3 to 4 foot
      - Deters casual trespasser
    - 6 to 7 foot
      - Too hard to climb easily
    - 8 foot with barbed wire
      - Deters intruders
  - Lighting
    - 8 feet high with 2 feet candle power
  - Locks
    - Preset locks
      - Mechanical
    - Programmable
      - Combination locks
  - CCTV
    - Visual surveillance
    - Record for analysis
    - Monitoring – Preventative controls
    - Recording – Detective control
- Facility Access Control Devices
  - Motion detectors
    - Wave Pattern
    - Capacitance
    - Audio Detectors
- Alarms
  - Local
    - Rings locally
  - Central
    - managed
  - Auxiliary Station Systems
    - Calls emergency services
- Data Destruction
  - Reformat 7 times according to TCSEC Orange Book standards
  - Shredders should cross cut

Define the threats to Physical Security

- Threats
  - Confidentiality
    - Unauthorized disclosure of information
    - Physical Theft
  - Integrity
    - Loss of control over the system
    - Physical Theft
  - Availability
    - Interruptions in providing computer services
    - Physical Damage
    - Physical Theft
- Major sources of Physical Loss
  - Temperature
  - Gases
  - Liquids
  - Organisms
  - Projectiles
  - Movement
  - Energy Anomalies

Discuss the Controls for Physical Security

- Controls for Physical Security
  - Administrative Controls
    - Requirements planning
      - Choosing a secure site
      - Walls
      - Ceilings
      - Floors
      - Windows
      - Doors
      - Sprinkler System
      - Liquid and gas lines
      - Air Con
      - Electrical requirements
      - Audit trails
    - Security Management
      - Emergency Procedures
        - Emergency Shutdown procedures
        - Evacuation procedures
        - Employee training
        - Periodic system tests
    - Personal Controls
  - Physical and technical controls
    - Control requirements
    - Access control; devices
    - Intrusion detection and alarms
    - Computer inventory control
    - Media storage requirements

MindCert.com
Utilize the power of your mind

Motivation and Study Techniques to help you learn, remember, and pass your technical exams!
- Cisco
- CISSP
- CEH
- More coming soon...

Visit us www.mindcert.com

Subscribe via RSS