Physical Security Requirements

Chapter 19

SYBEX

© SYBEX Inc. 2016. All Rights Reserved.

Apply Secure Principles to Site and Facility Design

- Secure facility plan
- Site selection
- Visibility
- Natural disasters
- Facility design

SYBEX

© SYBEX Inc. 2016. All Rights Reserved.

Secure Facility Plan

- Critical path analysis
- Security for basic requirements
- Technology convergence

SYBEX

© SYBEX Inc. 2016. All Rights Reserved.

Site Selection

- Cost
- Location
- Size
- Security requirements
- Preexisting structure or custom construction
- Proximity to others
- Weather conditions

© SYBEX Inc. 2016. All Rights Reserved.

Visibility

- Surrounding terrain
- Vehicle and foot traffic
- Residential, business, or industrial area
- Line of sight
- Crime rate
- Emergency services
- Unique local hazards

SYBEX

© SYBEX Inc. 2016. All Rights Reserved.

Natural Disasters

- Common local natural disasters
- Severe weather patterns
- Protection for workers and assets

SYBEX

© SYBEX Inc. 2016. All Rights Reserved.

Facility Design

- Based on level of security needs
- Combustibility, fire rating
- Construction materials
- Load rating
- Intrusion, emergency access, resistance to entry
- Security architecture
- CPTED

© SYBEX Inc. 2016. All Rights Reserved.

Design and Implement Physical Security

- Design concepts
- Equipment failure
- Wiring closets
- Server rooms
- Media storage facilities
- Evidence storage
- Restricted and work area security (e.g., operations centers)
- Datacenter security
- Utilities and HVAC considerations
- Water issues (e.g., leakage, flooding)
- Fire prevention, detection, and suppression

SYBEX

© SYBEX Inc. 2016. All Rights Reserved.

Design Concepts

- Administrative physical security controls
- Technical physical security controls
- Physical controls for physical security
- Corporate vs. personal property
- Deterrence
- Denial
- Detection
- Delay

SYBEX

© SYBEX Inc. 2016. All Rights Reserved.

Equipment Failure

- Failure is inevitible
- Purchase replacement parts as needed
- Onsite replacement warehousing
- SLA with vendors
- MTTF
- MTTR
- MTBF

SYBEX

© SYBEX Inc. 2016. All Rights Reserved.

Wiring Closets

- Premises wire distribution room
- Prevent physical unauthorized access
- Do not use as general storage
- Do not store flammable materials
- Use video surveillance
- Perform regular physical inspections

SYBEX

© SYBEX Inc. 2016. All Rights Reserved.

Server Rooms

- Need not be human compatible
- Support optimal operation of IT
- Locate in core of building
- One-hour minimum fire rating for walls

© SYBEX Inc. 2016. All Rights Reserved.

Media Storage Facilities

- Store blank, reusable, and installation media
- Data remnants
- Use a locked cabinet
- Have a librarian or custodian
- Check-in/check-out process
- Sanitization, zeroization

SYBEX

© SYBEX Inc. 2016. All Rights Reserved.

Evidence Storage

- Becoming important business task
- Drive images and virtual machine snapshots
- Distinct from production
- Block Internet access
- Track all activities
- Calculate hashes of all files
- Limit access
- Encrypt stored data

SYBEX

© SYBEX Inc. 2016. All Rights Reserved.

Restricted and Work Area Security

- Operations centers
- Distinct and controlled area access
- Walls or partitions
- Shoulder surfing
- Assign classifications
- Track assets with RFID

SYBEX

© SYBEX Inc. 2016. All Rights Reserved.

Datacenter Security

- Smart cards
- Proximity readers
- Intrusion detection systems
- Access abuses
- Emanation security

SYBEX

© SYBEX Inc. 2016. All Rights Reserved.

Utilities and HVAC Considerations

- UPSs
- Surge protectors
- Generators
- Fault, blackout, sag, brownout, spike, surge, inrush, noise, transient, clean, ground
- EMI vs. RFI
- Temperature, humidity, static

SYBEX

© SYBEX Inc. 2016. All Rights Reserved.

Water Issues

- Leakage
- Flooding
- Electrocution
- Water detection circuits
- Shutoff values
- Drainage locations

SYBEX

© SYBEX Inc. 2016. All Rights Reserved.

Fire Prevention, Detection, and Suppression

- **Fire triangle: fire, heat, oxygen, combustion**
- **Stages: Incipient, smoke, flame, heat**
- **Fire extinguisher classes**
- **Fire detection systems**
- **Water suppression**
  - Wet pipe, dry pipe, pre-action, deluge
- **Gas suppression**
  - CO2, Halon, FM-200, alternatives

SYBEX

© SYBEX Inc. 2016. All Rights Reserved.

Implement and Manage Physical Security

- Perimeter (e.g., access control and monitoring)
- Internal security (e.g., escort requirements/visitor control, keys, and locks)

SYBEX

© SYBEX Inc. 2016. All Rights Reserved.

Perimeter

- Fences
- Gates
- Turnstiles
- Mantraps
- Lighting
- Security guards and dogs

SYBEX

© SYBEX Inc. 2016. All Rights Reserved.

Internal Security

- **Keys and combination locks**
- **Electronic access control (EAC) locks**
- **Badges**
- **Motion detectors**
  - Infrared, heat, wave pattern, capacitance, photoelectric, passive audio
- **Intrusion alarms**
  - Deterrent alarms, repellant alarms, notification alarms
  - Local alarm, central station, auxiliary station

SYBEX

© SYBEX Inc. 2016. All Rights Reserved.

Internal Security

- Secondary verification mechanisms
- Environment and life safety
- Privacy responsibilities and legal requirements
- Regulatory requirements

SYBEX

© SYBEX Inc. 2016. All Rights Reserved.