1213 سبر
Network Defense

Lecture #9 Part 1

Implementing Controls to Protect Assets

Topics

- Comparing Physical Security Controls
- Adding Redundancy and Fault Tolerance
- Protecting Data with Backups
- Comparing Business Continuity Elements

Physical Security Controls

- Perimeter
- Buildings
- Secure work areas
- Server rooms
- Hardware (such as cable locks)

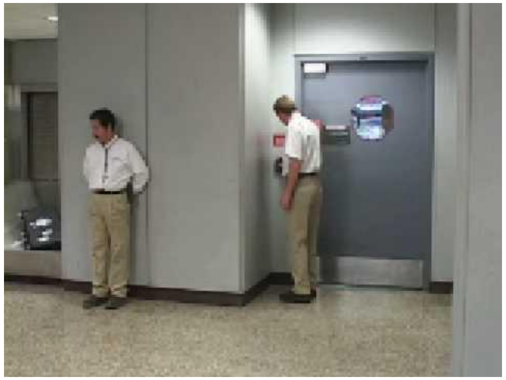
Physical Security Controls

- Door access systems
  - Proximity cards

- Locks
  - Physical locks
  - Physical cipher locks
  - Biometric locks
  - Cable locks

- Tailgating and access control vestibules

- Security guards



Physical Security Controls

Physical Security Controls

- Personnel
  - Two-person integrity
- Cameras

- Fencing, lighting, and alarms

Sensors

- Motion detection
- Noise detection
- Temperature
- Moisture detection
- Proximity reader
- Cards

- Barricades
  - Bollards
- Signage
- Drones

Physical Security Controls

Asset Management

- Architecture weaknesses
- Design weaknesses
- System sprawl
- Undocumented assets

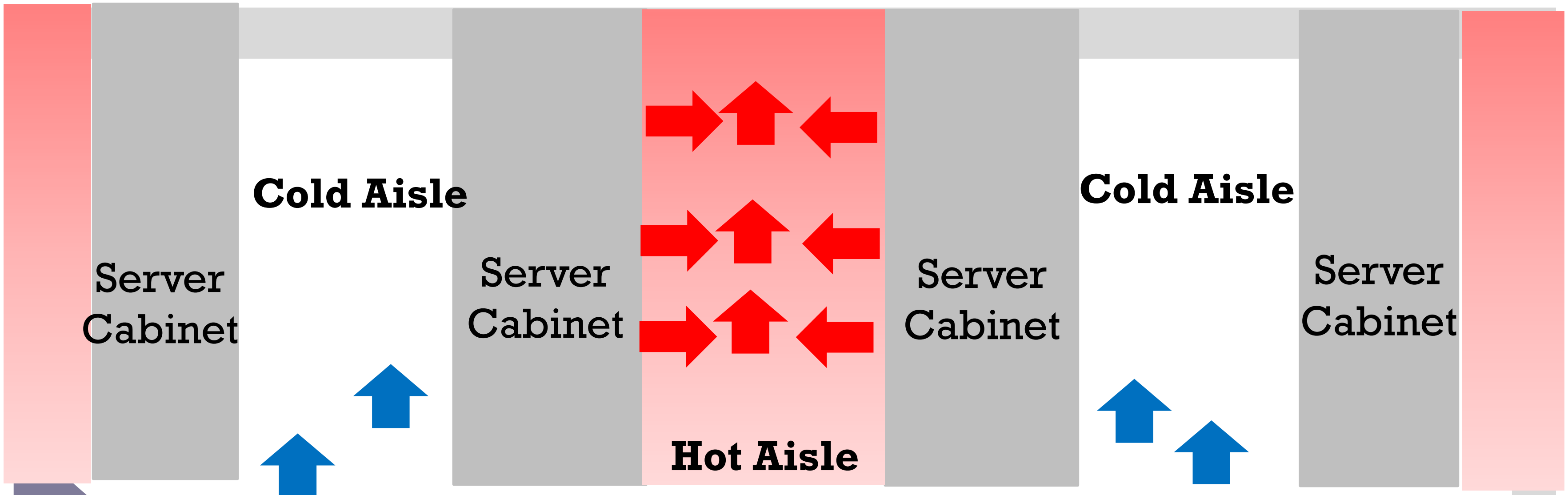
Diversity

- Defense in depth
  - Also known as layered security
- Vendor diversity
- Technology diversity
- Control diversity

Secure Areas

- Air gap
- Vaults
- Faraday Cage
- Safes

Environmental Controls



- Hot and cold aisles
  - Regulate the cooling

Physical Attacks

- **Malicious Universal Serial Bus (USB) cable**
- **Malicious flash drive**
- **Card skimming**
- **Card cloning**

Redundancy and Fault Tolerance

- Single point of failure
  - Any component whose failure results in the failure of an entire system
- Remove single points of failure with
  - RAID (disk)
  - Failover clustering (server)
  - UPS and generators (power)
  - Personnel
- Single points of failure are often overlooked until a disaster occurs

Disk Redundancies

- Inexpensive
- Adds fault tolerance and increases availability
- Hardware RAID more efficient than software RAID