Lesson 21

Explaining Physical Security

Topic 21A

Explain the Importance of Physical Site Security Controls

Syllabus Objectives Covered

- 1.2 Given a scenario, analyze potential indicators to determine the type of attack
- 2.7 Explain the importance of physical security controls

Physical Security Controls

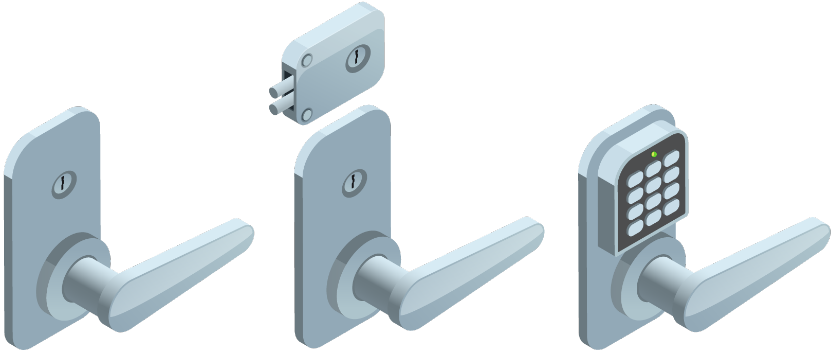
- Authentication
  - Create access lists and identification mechanisms to allow approved persons through barriers
- Authorization
  - Create barriers around a resource so that access can be controlled through defined entry and exit points
- Accounting
  - Keep a record of when entry/exit points are used and detect security breaches

Site Layout, Fencing, and Lighting

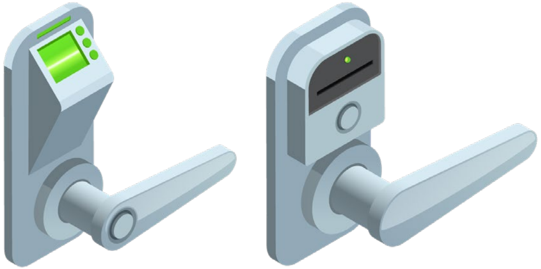
- Site layout
  - Zone-based design to accommodate traffic flows and surveillance
  - Signage
  - Industrial camouflage
- Barricades and entry/exit points
  - Bollards
- Fencing
- Lighting
  - Make staff feel secure
  - Assist surveillance

Gateways and Locks

- Lock types
  - Physical (conventional/deadbolt)
  - Electronic
    - Cipher/combination
    - Magnetic swipe card
    - Smart card/proximity reader
  - Biometric
- Access control vestibules/mantraps and turnstiles
- Cable locks



Images from user macrovector © 123RF.com.



Images from user macrovector © 123RF.com.

Physical Attacks Against Smart Cards and USB

- Smart card attacks
  - Cloning
  - Skimming
  - Card types and vulnerability level
- Malicious USB/juice-jacking
  - USB data blocker

Alarm and Sensor Systems

- Circuit
  - Open or closed
  - Detect intrusion through a barrier
- Motion detection
  - Radar or infrared
  - Detect intrusion in a space
- Noise detection
- Proximity readers
- Duress
  - Fixed or mobile

Security Guards and Cameras

Image by Dario Lo Presti © 123RF.com.

- Security guards
  - Police entry points
  - Operate surveillance mechanisms
  - Respond to alarms
- Remote surveillance and monitoring
  - Video/CCTV
  - Motion recognition
  - Object detection
  - Robot sentries
  - Drones/UAV

Reception Personnel and ID Badges

- Challenge policy
- Reception personnel and visitor logs
  - Sign-in/sign-out
  - Visitor information
- Two-person integrity/control
- ID badges

Topic 21B

Explain the Importance of Physical Host Security Controls

Syllabus Objectives Covered

- 2.7 Explain the importance of physical security controls
- 4.1 Given a scenario, use the appropriate tool to assess organizational security (Data sanitization only)

Secure Areas

- Server rooms and data centers
- Lockable cabinets
- Colocation cages
- Air gaps and demilitarized zones
- Safes
- Vaults

Image © 123RF.com.

Image © 123RF.com.

Image © Chris Dag and shared with CC BY 2.0 flickr.com/photos/chrisdag/865711871.

Protected Distribution and Faraday Cages

- Protected cable distribution/protected distribution system (PDS)
  - Prevent eavesdropping
  - Prevent/delay cable cutting DoS
- Faraday cage
  - Transient Electromagnetic Pulse Emanation Standard (TEMPEST)

Heating, Ventilation, Air Conditioning

- Cooling/warming, humidity, dust control
- Optimum temperature and humidity levels
  - Moisture detection sensors
  - Temperature detection sensors
- HVAC sizing
  - Equipment wattage
  - British Thermal Units (BTU)/hour
- Air flow
- Positive air pressure to remove contaminants

Hot and Cold Aisles

- Optimize air flow
- Place servers back-to-back
- Hot aisle/cold aisle
- Do not allow contamination of cooled air by warmed air

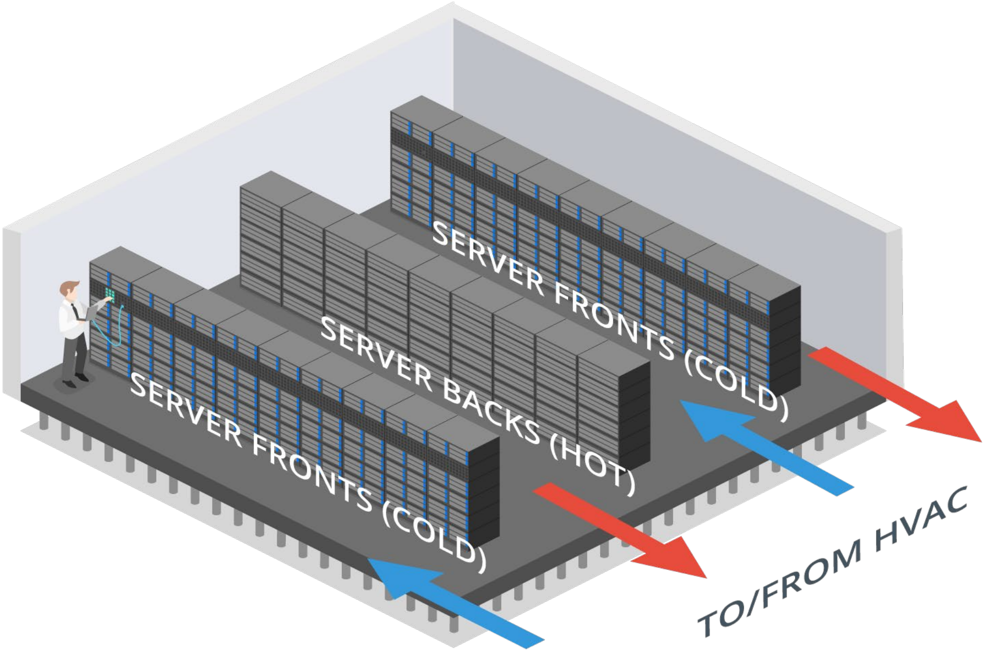


Image © 123RF.com.

Fire Detection and Suppression

- Fire safety
  - Fire exits and evacuation procedures
  - Fire-resistant building design
  - Smoke/flame detectors/alarms
- Personal fire extinguishers
  - Class C for use around electrical hazard
- Sprinklers
  - Dry pipe
  - Pre-action
  - Halon
  - Clean Agent

Secure Data Destruction

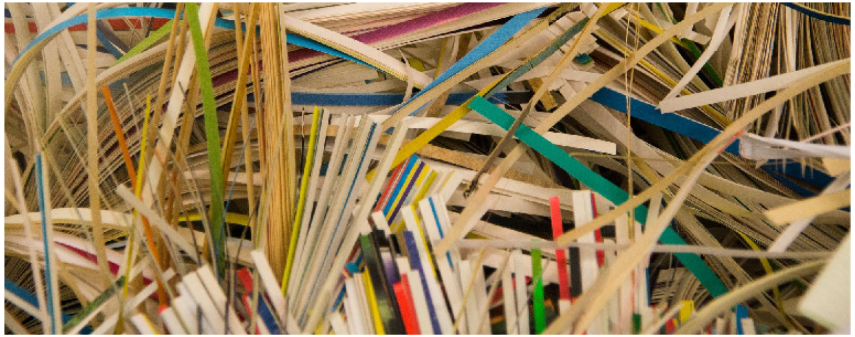
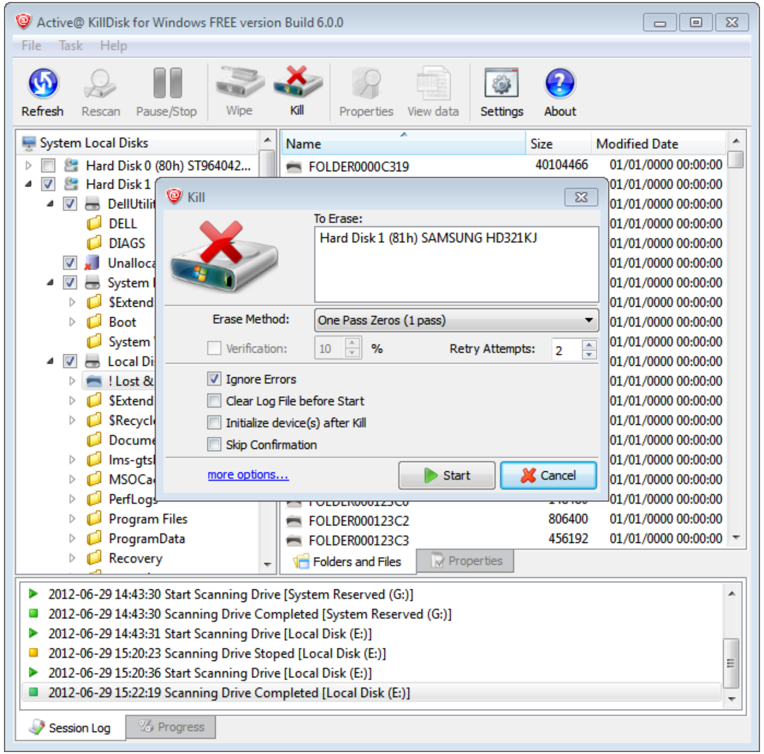


Photo by monsterkoi on Pixabay.

- Media sanitization/remnant removal
- Physical destruction
  - Burning/incineration
  - Shredding/pulping
  - Pulverizing
  - Degaussing
- Use of third-parties and certificates of destruction

Data Sanitization Tools



Name	Size	Modified Date
FOLDER0000C319	40104466	01/01/0000 00:00:00
FOLDER000123C2	806400	01/01/0000 00:00:00
FOLDER000123C3	456192	01/01/0000 00:00:00

To Erase: Hard Disk 1 (81h) SAMSUNG HD321KJ

Erase Method: One Pass Zeros (1 pass)

☐ Verification: 10 %

Retry Attempts: 2

☑ Ignore Errors

☐ Clear Log File before Start

☐ Initialize device(s) after Kill

☐ Skip Confirmation

```
2012-06-29 14:43:30 Start Scanning Drive [System Reserved (G:)]
2012-06-29 14:43:30 Scanning Drive Completed [System Reserved (G:)]
2012-06-29 14:43:31 Start Scanning Drive [Local Disk (E:)]
2012-06-29 15:20:23 Scanning Drive Stoped [Local Disk (E:)]
2012-06-29 15:20:36 Start Scanning Drive [Local Disk (E:)]
2012-06-29 15:22:19 Scanning Drive Completed [Local Disk (E:)]
```

Screenshot used with permission from LSoft Technologies, Inc.

- Secure disposal of electronic data remnants
- Overwriting/disk wiping
  - Zero filling
  - Multiple passes
- Secure Erase (SE)
  - Hard disk drives (HDD)
  - Solid state drives (SSD)/flash media
- Instant Secure Erase (ISE)/crypto erase
  - Self-encrypting drives (SED)
  - Delete media encryption key

Lesson 21

Summary