

# IT 4823

## Information Security Administration

### Physical and Infrastructure Security

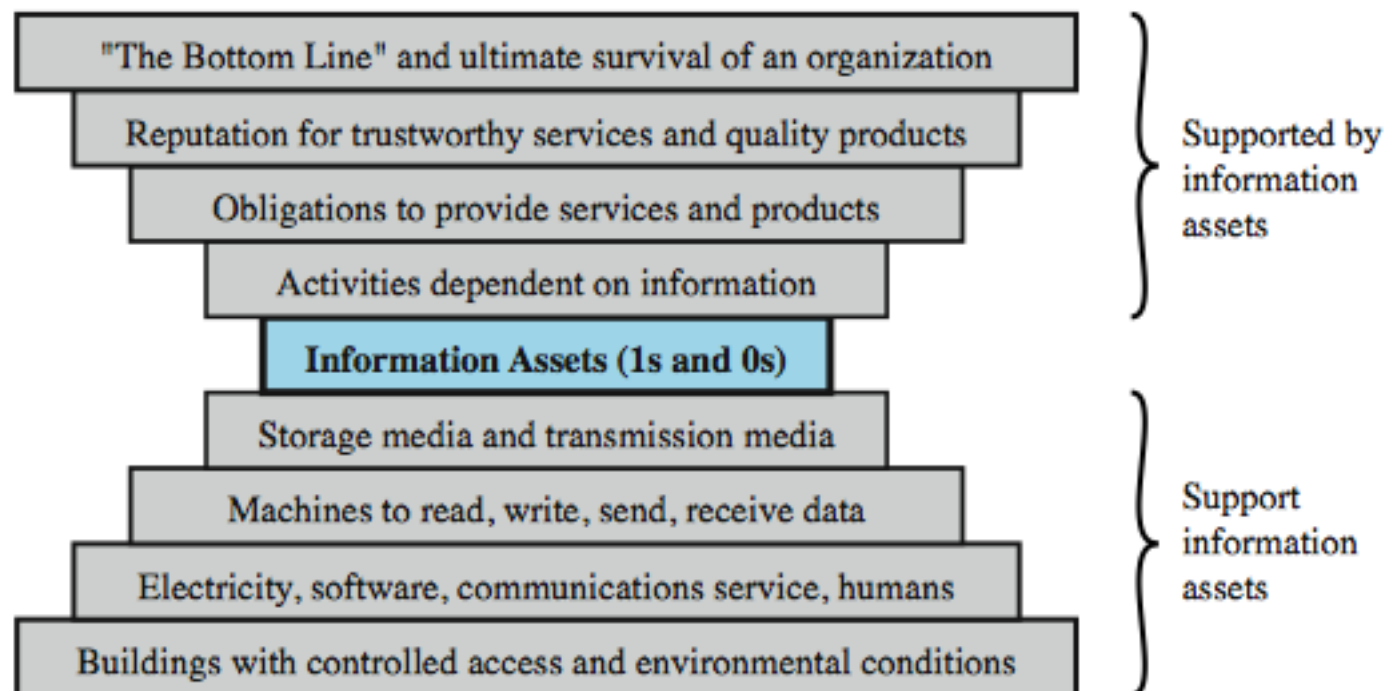


Notice: This session  
is being recorded.

# Physical Security

- Physical security addresses design, implementation, and maintenance of countermeasures that protect physical resources of an organization.
- Most controls can be circumvented if an attacker gains physical access.
- Physical security is as important as logical security.

# Physical Security Context



# Major Sources of Physical Loss

- People (!)
- Extreme temperature
- Gases
- Liquids
- Living organisms
- Projectiles
- Movement
- Energy anomalies

*From Donn B. Parker*

# Physical Security Threats

We can group these threats:

- Environmental threats (including natural disasters)
- Technical threats
- Human-caused threats, both malicious and accidental.

# Forces of Nature

- Wind (tornado, hurricane)
  - Location
  - Construction
- Flood
  - Location
- Electrical storms
  - Power redundancy
  - Construction
  - Location
- Ice storm, blizzard
  - Location
  - Construction
- Earthquake
  - Location
  - Construction
- Extremes of heat and cold
  - HVAC

# Environmental Threats

- Inappropriate temperature and humidity
- Fire and smoke
- Water
- Chemical, radiological, biological hazards
- Dust (especially paper dust)
- Infestation (mold, insects, vermin)

# Technical Threats

- Electric power is essential to run equipment
  - power utility problems:
    - under-voltage - dips/brownouts/outages, interrupt service
    - over-voltage - surges/faults/lightening, can destroy chips
    - noise - on power lines, may interfere with device operation
- Electromagnetic interference (EMI)
  - from line noise, motors, fans, heavy equipment, other computers, nearby radio stations and microwave relays
  - can cause intermittent problems with computers



# Human-Caused Threats

- Less predictable, may be targeted, harder to deal with
- Include:
  - unauthorized physical access leading to other threats
  - theft of equipment / data
  - vandalism of equipment / data
  - misuse of resources

# Mitigation Measures for Environmental Threats

- Inappropriate temperature and humidity
  - environmental control equipment, power
- Fire and smoke
  - alarms, preventive measures, fire mitigation
  - smoke detectors, no-smoking policy, housekeeping
- Water
  - manage lines, equipment location, cutoff sensors
- Other threats
  - appropriate technical counter-measures, limit dust entry, pest control

# Mitigation Measures for Technical Threats

- Electric power for critical equipment use
  - Uninterruptible power supply (UPS)
  - Emergency power generator
- Electromagnetic interference (EMI)
  - Filters and shielding
  - Dedicated circuits

# Mitigation Measures for Human-Caused Threats

- Physical access control
  - IT equipment, wiring, power, communications, media
- Several areas to consider
  - restrict building access, locked area, secured, power switch secured, tracking devices for portable equipment
- Intruder sensors / alarms

# Management Roles

- General management: responsible for facility security
- IT management and professionals: responsible for environmental and access security
- Information security management and professionals: perform risk assessments and implementation reviews; implement technical controls.

# Physical Access Controls

- *Secure facility*: a physical location engineered with controls designed to minimize risk from physical threats
- A secure facility can take advantage of natural terrain, traffic flow, and degree of urban development; can complement these with protection mechanisms (fences, gates, walls, guards, alarms)

# Computer Rooms, Wiring Closets

- Require special attention to ensure confidentiality, integrity, and availability of information
- Many logical controls are easily defeated if attacker gains physical access to computing equipment

# Protecting the Secure Facility

- **Physical Barriers**

- Exterior walls, fencing, and gates
- Locks and keys
- Interior walls

- **Identification**

- ID Cards and badges

- **Monitoring**

Electronic monitoring  
Alarm systems

- **Human (and animal) Barriers**

Guards

Dogs



# ID Cards and Badges

- Ties physical security with information access control
  - ID card is typically concealed
  - Name badge is visible
- Serve as simple form of biometrics (facial recognition)
- Should not be only means of control as cards can be easily duplicated, stolen, and modified
- Tailgating occurs when unauthorized individual follows authorized user through the control

# Locks and Keys

- Two types of locks: mechanical and electromechanical
- Locks can also be divided into four categories: manual, programmable, electronic, biometric
- Locks can fail; alternative procedures for controlling access must be put in place
- Locks fail in one of two ways
  - Fail-safe (open) lock
  - Fail-secure lock
- Fail-secure locks may violate fire codes

# Electronic Monitoring

- Records events where other types of physical controls are impractical or incomplete
- May use cameras with video recorders; includes closed-circuit television (CCT) systems
- Drawbacks
  - Reactive; do not prevent access or prohibited activity
  - Recordings often not monitored in real time; must be reviewed to have any value
- Some monitors can call attention to changes in real time

# Alarms and Alarm Systems

- Alarm systems notify monitoring station when an event occurs
- Detect fire, intrusion, environmental disturbance, or an interruption in services
- Rely on sensors that detect event; *e.g.*, motion detectors, smoke detectors, thermal detectors, glass breakage detectors, weight sensors, contact sensors, vibration sensors

# Alarm Monitoring

- Audible alarms
  - Rely on “whoever’s close by” to take action
  - May have deterrent value as burglar/intrusion alarms
- Auto-dialers
  - Call one or more numbers with a pre-programmed message
  - Direct police/fire calls generally not permitted
- Remote monitoring (service or in-house)

# Interior Walls and Doors

- Information asset security are sometimes compromised by construction of facility walls and doors
- Facility walls typically either standard interior wall or fire-rated wall
- High-security areas must have firewall-grade or masonry walls to provide physical security from potential intruders and improve resistance to fires
- Doors allowing access to high security rooms should be evaluated
- Recommended that push or crash bars be installed on computer rooms and closets

# Fire Security and Safety

- A serious threat to safety of people who work in an organization is possibility of fire.
- Fires account for substantial property damage, personal injury, and death.
- Imperative that physical security plans examine and implement strong measures to prevent, detect, and respond to fires.

# Fire Prevention

- Smoking policy
- Good housekeeping
- Policy on portable electric heaters
- Equipment maintenance, especially of portable equipment.



# Fire Detection and Response

- Fire suppression systems: devices installed and maintained to detect and respond to a fire
- Deny an environment of heat, fuel, or oxygen
  - Water and water mist systems
  - Carbon dioxide systems
  - Soda acid systems
  - Gas-based systems

# Fire Detection

- Fire detection systems fall into two general categories: manual and automatic
- Part of a complete fire safety program includes individuals who monitor chaos of fire evacuation to prevent an attacker accessing offices
- There are three basic types of fire detection systems: thermal detection, smoke detection, flame detection

# Fire Suppression

- Systems consist of portable, manual, or automatic apparatus
- Portable extinguishers are rated by the type of fire: Class A, Class B, Class C, Class D
- Installed systems apply suppressive agents; usually either sprinkler or gas systems

# Gas Emission Systems

- Until recently, two types of systems: carbon dioxide and Halon
- Carbon dioxide robs a fire of oxygen supply (but is dangerous as h ... well, it's dangerous because it can silently kill people!)
- Halon is clean but has been classified as ozone-depleting substance; new installations are prohibited
- Alternative “clean” agents include FM-200, Inergen, FE-13 (trifluoromethane)

# Failure Of Supporting Utilities

- Supporting utilities (heating, ventilation and air conditioning; power; water; and others) have significant impact on continued safe operation of a facility
- Each utility must be properly managed to prevent potential damage to information and information systems

# Utilities

- Heating, ventilation, air conditioning
  - Computer area
  - Remainder of building
- Electric power
- Water and sewer service
- Natural gas
- Transportation

# Heating, Ventilation, and Air Conditioning

HVAC systems control:

- Temperature
- Filtration
- Humidity (and static electricity)

# Specifying HVAC

- Multiple smaller units
- N+1 redundancy, at least
- Size for extreme ambient temperatures (both low and high)
- Consider the increasing density of equipment
- In cold climates, consider “economizing” systems
- Don’t forget emergency power for the HVAC



# Ventilation Shafts

- While ductwork is small in residential buildings, in large commercial buildings it can be large enough for individual to climb though
- If vents are large, install wire mesh grids at various points to compartmentalize the runs

# Water Problems

- Lack of water poses problem to systems, including functionality of fire suppression systems and ability of water chillers to provide air conditioning
- Surplus of water, or water pressure, poses a real threat (flooding; leaks)
  - No pipes (except sprinklers) within computer rooms
  - Under-floor water detection
- Very important to integrate water detection systems into alarm systems that regulate overall facilities operations

# Structural Collapse

- Unavoidable forces (earthquake, explosion, physical attack) can cause failures of structures that house organization
- Structures are designed and constructed with specific load limits; overloading these limits results in structural failure and potential injury or loss of life
- Periodic inspections by qualified civil engineers assist in identifying potentially dangerous structural conditions

# Interception of Data

- Three methods of data interception
  - Direct observation
  - Interception of data transmission
  - Electromagnetic interception
- U.S. government developed TEMPEST program to reduce risk of electromagnetic radiation (EMR) monitoring

# Mobile and Portable Systems

- With the increased threat to information security for laptops, tablets, and smart phones, mobile computing requires more security than average in-house system.
- Many mobile computing systems have corporate information stored within them; some are configured to facilitate user's access into organization's secure computing facilities.
- Theft of laptops, phones, etc. is a major risk

# Remote Computing Security

- Remote site computing: away from organizational facility
- Telecommuting: computing using telecommunications including Internet, dial-up, or leased point-to-point links
- Employees may need to access networks on business trips; telecommuters need access from home systems or satellite offices
- To provide secure extension of organization's internal networks, all external connections and systems must be secured

# In-House or Outsourced?

- Many qualified and professional agencies
- Benefit of outsourcing includes gaining experience and knowledge of agencies
- Downside includes high expense, loss of control over individual components, and level of trust that must be placed in another company

# Inventory Management

- Computing equipment should be inventoried and inspected on a regular basis
- Classified information should also be inventoried and managed
- Physical security of computing equipment, data storage media and classified documents varies for each organization



# Questions

