CSE 543
Information Assurance and Security

Physical and Personnel Security for Information Systems

Professor Stephen S. Yau

Importance of Physical Security

- Most focus on protecting ***data and logical systems***
- The ***physical systems*** (computer hardware) to run the programs and data must be protected
  - Physical security deals with who have access to buildings, computer rooms, and the devices within them
  - Protect sites from ***natural and man-made physical*** threats

Physical Security Threats

- **Weather**
  - Tornadoes, hurricanes, floods, fire, snow, ice, heat, cold, humidity
- **Fire/chemical**
  - Explosions, toxic waste/gases, smoke, fire
- **Earth movement**
  - Earthquakes, mudslides, tsunami
- **Structural failure**
  - Building collapse due to snow/ice/load weight, or moving objects (cars, trucks, airplanes, etc.)

Physical Security Threats (Cont.)

- **Energy**
  - Loss of power, radiation, magnetic wave interference,
- **Biological**
  - Virus, bacteria
- **Human**
  - Strikes, theft, sabotage, terrorism and war

Physical Security Areas

- Administrative controls
- Physical security controls
- Technical controls
- Environmental/life-safety controls
- Educating personnel

Administrative Controls

- **Restricting Work Areas**
  - Identify access rights to the ***site in general***
  - Decide various access rights ***required by each location*** (rooms, elevators, buildings) within the site
- **Escort Requirements and Visitor Control**
  - In many government facilities or facilities with strong government ties, ***foreign nationals*** are not allowed unescorted access to any site within the facility. Escorted access requires ***background clearance and onsite identity check***
  - For less secure sites, each visitor must have a clear ***purpose for visit and a confirmed contact*** within the site. A temporary badge will be given after the visitor sign-in at the security desk

Administrative Controls *(cont.)*

- **Site Selection**
  - **Visibility**
    - Most data centers are not descriptive, and do not advertise what they are and attract undue attention
  - **Locale considerations**
    - Neighborhood, local ordinances and variances, crime rate, hazardous sites nearby, such as landfills, waste dumps, and nuclear reactors.
  - **High Probability for Natural disasters**
  - **Transportation**
    - Airport, highways, railroads, etc.

Physical Security Controls

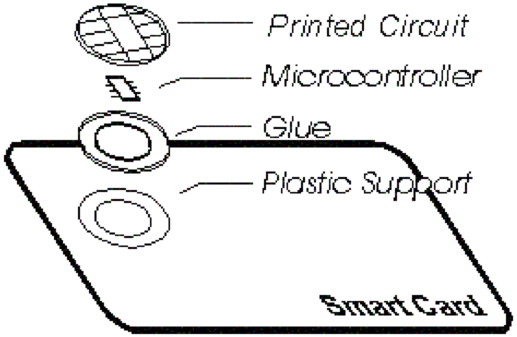
- **Perimeter Security Controls**
  - Gates, fences, turnstiles, mantraps
- **Badging**
  - Photo identification that not only authenticates an individual, but also continues to identify the individual while inside the facility

Physical Security Controls (Cont.)

- **Keys and Combination Locks**
  - Mechanical locks , password locks, electronic locks, etc.
- **Security Dogs**
  - Well-trained dogs are good at detecting intruders or sniffing out explosives
- **Lighting**
  - Proper lighting could serve as a deterrent

Technical Controls

- **Smart card**
  - Semiconductor chip with logic and nonvolatile memory
  - Software that detects unauthorized tampering and intrusions to the chip and if detected, can lock or destroy the contents of the chip to prevent disclosure or unauthorized uses
  - Three major types: contact, contact-less and combinations of the two.



Technical Controls (Cont.)

- **Audit Trails/Access Logs**
- **Physical Intrusion Detection**
  - Metallic foil tape, infrared light beams, motion sensors
- **Alarm Systems**
  - Systems like ADT, monitoring and responding to intrusion alert
- **Biometrics**

Environmental/Life-safety Controls

- **Power**
  - ***Power-outage***: Emergency lights and continuing functioning of those electronic gates are needed
  - ***Uninterrupted power***: Uninterrupted Power Service (UPS) and emergency power-off switch
  - ***Constant voltage and current: Regulator***

Environmental/ Life-safety Controls *(Cont.)*

- **Fire/Chemical Detection and Suppression**
  - *Targets*: Explosions, toxic waste/gases, smoke, fire
  - ***Detectors:*** Heat sensor, flame detector, smoke detector
  - ***Extinguishing systems***: Water-sprinkler or gas-discharge system
- **Heating, Ventilation and Air Conditioning**

Educating Personnel

- **Security staff** should be prepared for ***potential of unforeseen acts***
- **Other employees** should be reminded ***periodically*** of ***importance of helping their surroundings secure***
  - Being mindful of ***physical and environmental considerations*** required to protect information systems
  - Adhering to ***emergency and disaster plans***
  - ***Monitoring unauthorized use*** of equipment and services, and ***reporting*** those activities to security personnel
  - ***Recognizing security objectives*** of organization
  - ***Accepting individual responsibilities*** associated with their jobs and that of their coworkers

What Is Personnel Security?

- Security mechanisms reducing risks of human errors, thefts, frauds or misuse of facilities within an organization
- Not just an IT issue
  - ***Human Resource (HR)*** is the main player
  - Cross reference (refer to other organizations' IA in HR) and provide input to HR policies

Types of Implementation

- ***Background checks***
- ***Security clearances***
- ***Employment agreements***
- ***Hiring and termination practices***
- *Job descriptions*
- ***Job rotation***
- ***Separation of duties and responsibilities***

Background Checks

- Personnel controlling IT resources
  - Security Personnel
  - Net Administrators
  - Managers
  - Auditors
- Support hiring decisions
- Provide some protection and assurance

Background Checks *(Cont.)*

- What can be checked on an applicant?
  - Credit (financial) report
  - SSN searches
  - Workers compensation reports
  - Criminal record
  - Motor vehicle report
  - Education verification
  - Reference checks
  - Prior employment verification

Security Clearances

- Applicable to
  - Uniformed members of the military
  - Civilian employees working for government agencies
  - Employees of government contractors

Employment Agreements

- ***Non-competitive:***
  - Will not compete with your employer by engaging in any business of similar nature as an employee, independent contractor, owner, partner, significant investor, etc.
  - May broadly limit from working in same field, even if employee does not work for a direct competitor. May restrict in both time and locations

Employment Agreements *(Cont.)*

- ***Non-disclosure:***
  - Used when employer with unpatented ideas wants employees to maintain the idea confidential
  - Restricts dissemination of corporate information to unauthorized entities, especially competitors, press, analysts, and foreign agents

Hiring and Termination Practices

- Strict HR policies
- Hiring manager responsible for review of background checks
- Managers must take ***timely and appropriate disciplinary actions***
- Applicable to contractors/sub-contractors.

Hiring and Termination Practices (Cont.)

- From IT perspective
  - Starting/closing accounts
  - Notifying employee of account information
  - Forwarding e-mail and voice-mail
  - Changing locks and number-combinations
  - Changing system passwords
  - Notifying all personnel

Job Descriptions

- Based on designated position sensitivity
- Based on sensitivity of information handled
- Addressing security responsibilities of the position
- Considered in performance evaluation

Job Rotation

- Implemented where feasible
  - Discourages ***fraud, waste, and abuse***
  - Discourages ***collusion*** (secret agreement or cooperation especially for illegal or deceitful purpose)
  - Promotes ***cross-training***
  - Often not possible in highly specialized jobs

Separation of Duties

- Ensure people *checking* for inappropriate use of IT resources
- No one individual should be responsible for completing a task involving sensitive, valuable, or critical information from beginning to end
- A person must not be responsible for approving his/her own work
- What to separate?
  - Security from audit
  - Accounts payable from accounts receivable
  - Development from production

Summary

- Make sure to hire ***"good employees"*** as much as possible, i.e. ***competent, honest, and dependable***
- Make sure employees know their ***responsibilities***
- Encourage being ***good employees***
- Know how to handle ***if good employees are discovered to turn bad***