Chapter 5
Physical and Infrastructure Security

Book Reading: Computer Security Principles and Practice (3ed), 2015, p.534-554

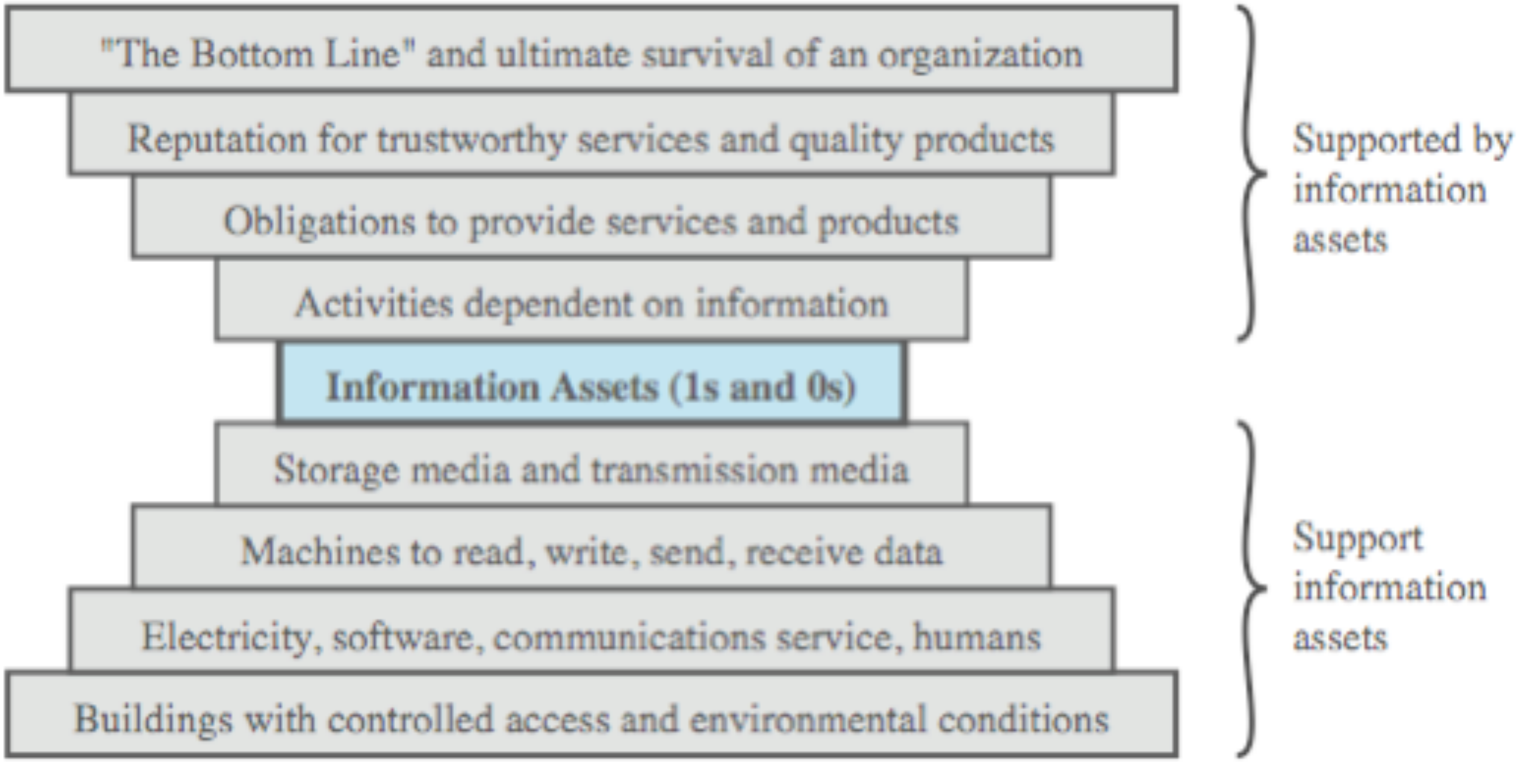
Physical and Infrastructure Security

- **Logical security**: Protects computer-based data from software-based and communication-based threats
- **Physical security** (also called infrastructure security)
  - Protects the information systems that contain data and the people who use, operate, and maintain the systems
  - Must prevent any type of physical access or intrusion that can compromise logical security
- **Premises security (**also known as corporate or facilities security)
  - Protects the people and property within an entire area, facility, or building(s), and is usually required by laws, regulations, and fiduciary obligations
  - Provides perimeter security, access control, smoke and fire detection, fire suppression, some environmental protection, and usually surveillance systems, alarms, and guards

Physical Security

- Protect physical assets that support the storage and processing of information
- Involves two complementary requirements
  - **Prevent damage to physical infrastructure**: information system hardware, physical facility, supporting facilities, personnel
  - **Prevent physical infrastructure misuse leading to misuse/damage of protected information** (e.g., vandalism, theft, copying, unauthorized entry, …)

Physical Security Context



"The Bottom Line" and ultimate survival of an organization

Reputation for trustworthy services and quality products

Obligations to provide services and products

Activities dependent on information

Information Assets (1s and 0s)

Storage media and transmission media

Machines to read, write, send, receive data

Electricity, software, communications service, humans

Buildings with controlled access and environmental conditions

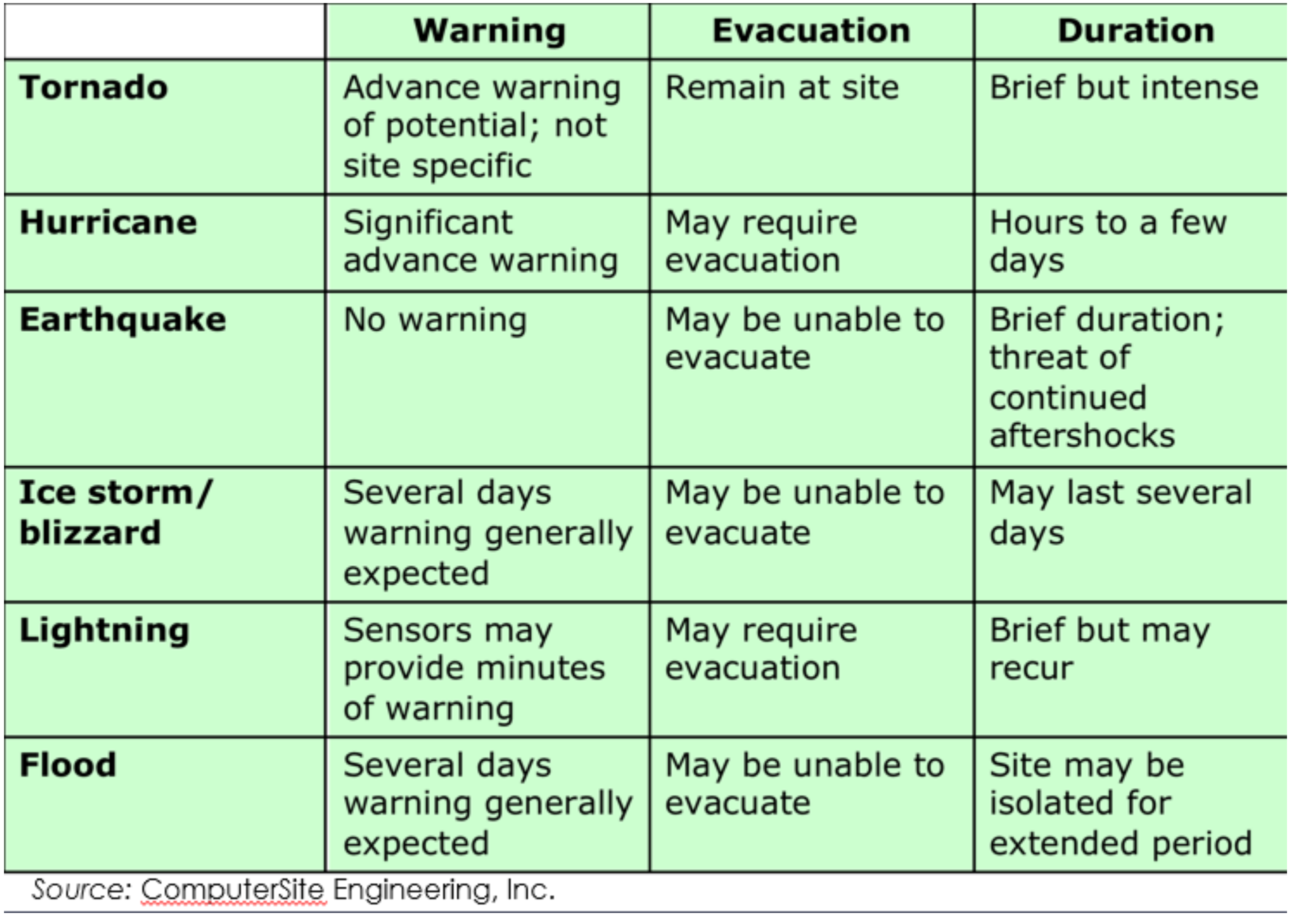
Supported by information assets

Support information assets

Physical Security Threats

- Physical situations and occurrences that threaten information systems
  - Natural disasters
  - Environmental threats (e.g., heat)
  - Technical threats
  - Human-caused threats

Characteristics of Natural Disasters



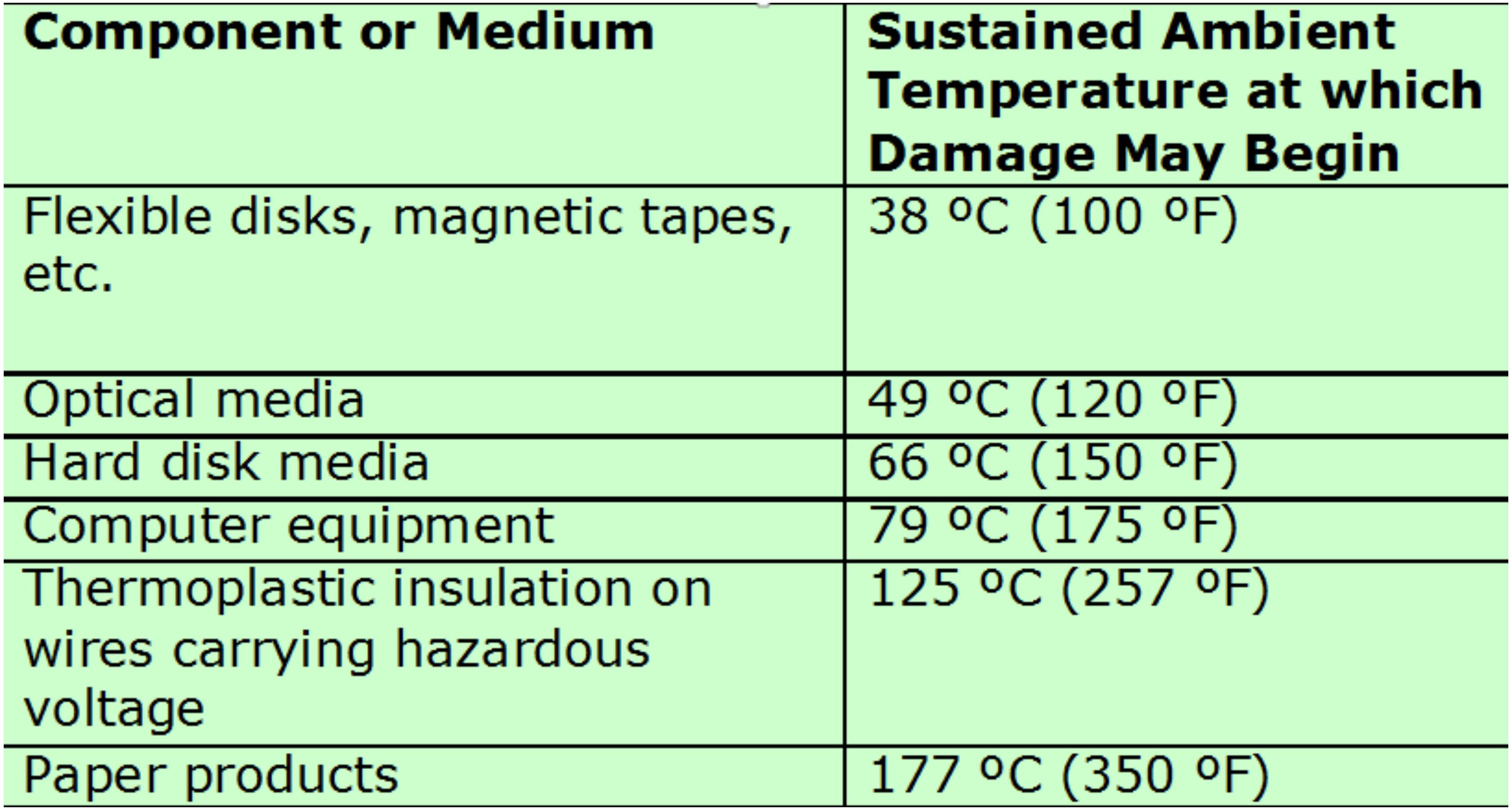
	Warning	Evacuation	Duration
Tornado	Advance warning of potential; not site specific	Remain at site	Brief but intense
Hurricane	Significant advance warning	May require evacuation	Hours to a few days
Earthquake	No warning	May be unable to evacuate	Brief duration; threat of continued aftershocks
Ice storm/ blizzard	Several days warning generally expected	May be unable to evacuate	May last several days
Lightning	Sensors may provide minutes of warning	May require evacuation	Brief but may recur
Flood	Several days warning generally expected	May be unable to evacuate	Site may be isolated for extended period

Source: ComputerSite Engineering, Inc.

Environmental Threats

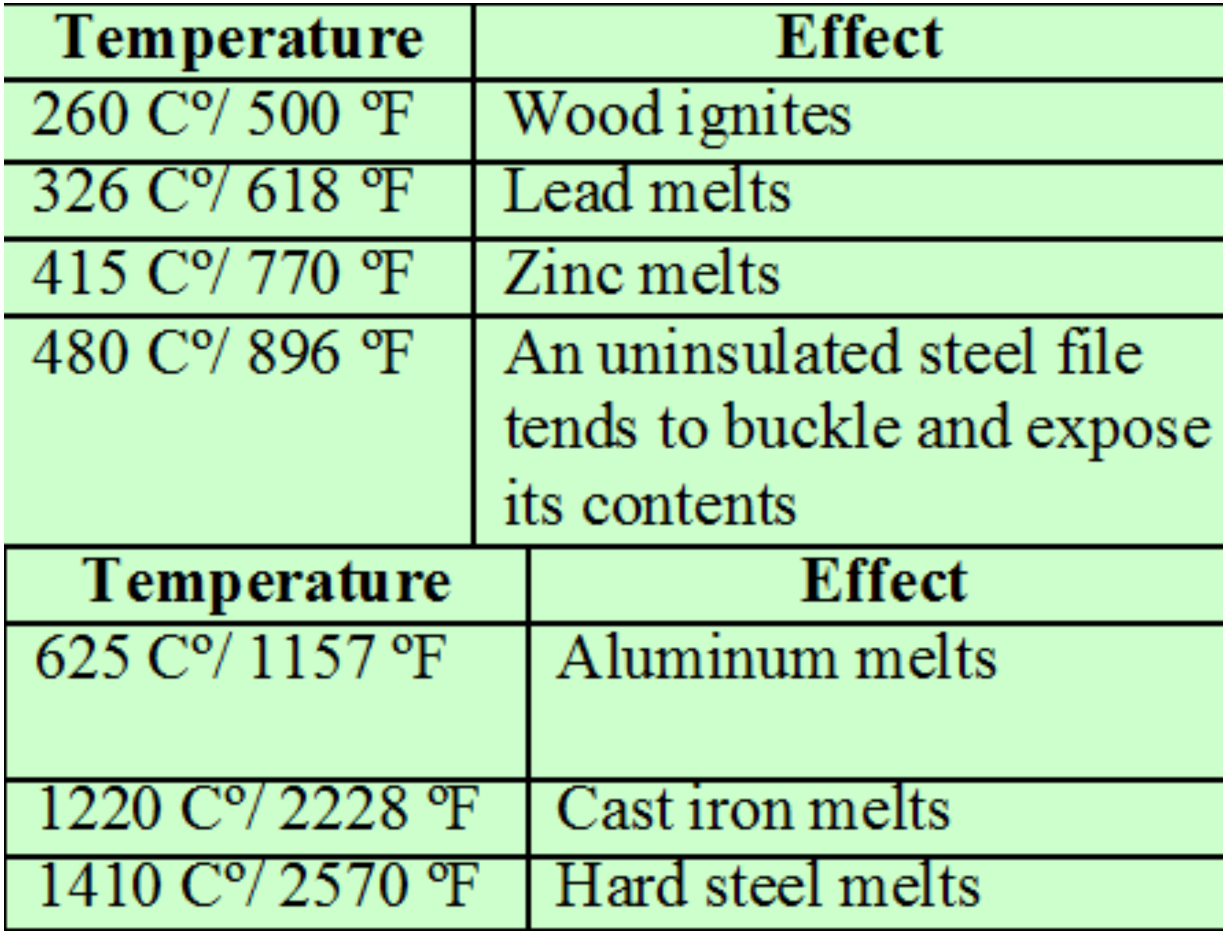
- Inappropriate temperature and humidity
- Fire and smoke
- Water
- Chemical, radiological, biological hazards
- Dust
- Infestation

Temperature Thresholds for Damage to Computing Resources



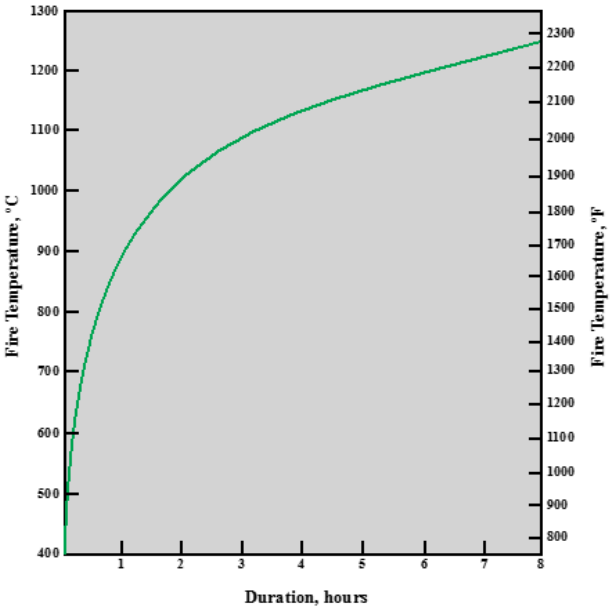
Component or Medium	Sustained Ambient Temperature at which Damage May Begin
Flexible disks, magnetic tapes, etc.	38 °C (100 °F)
Optical media	49 °C (120 °F)
Hard disk media	66 °C (150 °F)
Computer equipment	79 °C (175 °F)
Thermoplastic insulation on wires carrying hazardous voltage	125 °C (257 °F)
Paper products	177 °C (350 °F)

Temperature Effects



Temperature	Effect
260 C°/ 500 °F	Wood ignites
326 C°/ 618 °F	Lead melts
415 C°/ 770 °F	Zinc melts
480 C°/ 896 °F	An uninsulated steel file tends to buckle and expose its contents

Temperature	Effect
625 C°/ 1157 °F	Aluminum melts
1220 C°/ 2228 °F	Cast iron melts
1410 C°/ 2570 °F	Hard steel melts



Technical Threats

- Electrical 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 & 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 Environmental Threats

- Inappropriate temperature and humidity
  - Environmental control equipment, power
- Fire and smoke
  - Alarms, preventative measures, fire mitigation
  - Smoke detectors, no smoking
- Water
  - Manage lines, equipment location, cutoff sensors
- Other threats: limit dust entry, pest control

Mitigation Measures
Technical Threats

- Electrical power for critical equipment use
  - Use uninterruptible power supply (UPS)
  - Emergency power generator
- Electromagnetic interference (EMI)
  - Filters and shielding

Mitigation Measures Human-Caused Threats

- Physical access control
  - IT equipment, wiring, power, comms, media
- Have a spectrum of approaches
  - Restrict building access, locked area, secured, power switch secured, tracking device
- Also need intruder sensors/alarms

Recovery from Physical Security Breaches

- Redundancy
  - To provide recovery from loss of data
  - Ideally off-site, updated as often as feasible
  - Can use batch encrypted remote backup
  - Extreme: remote hot-site with live data
- Physical equipment damage recovery
  - Depends on nature of damage and cleanup
  - May need disaster recovery specialists

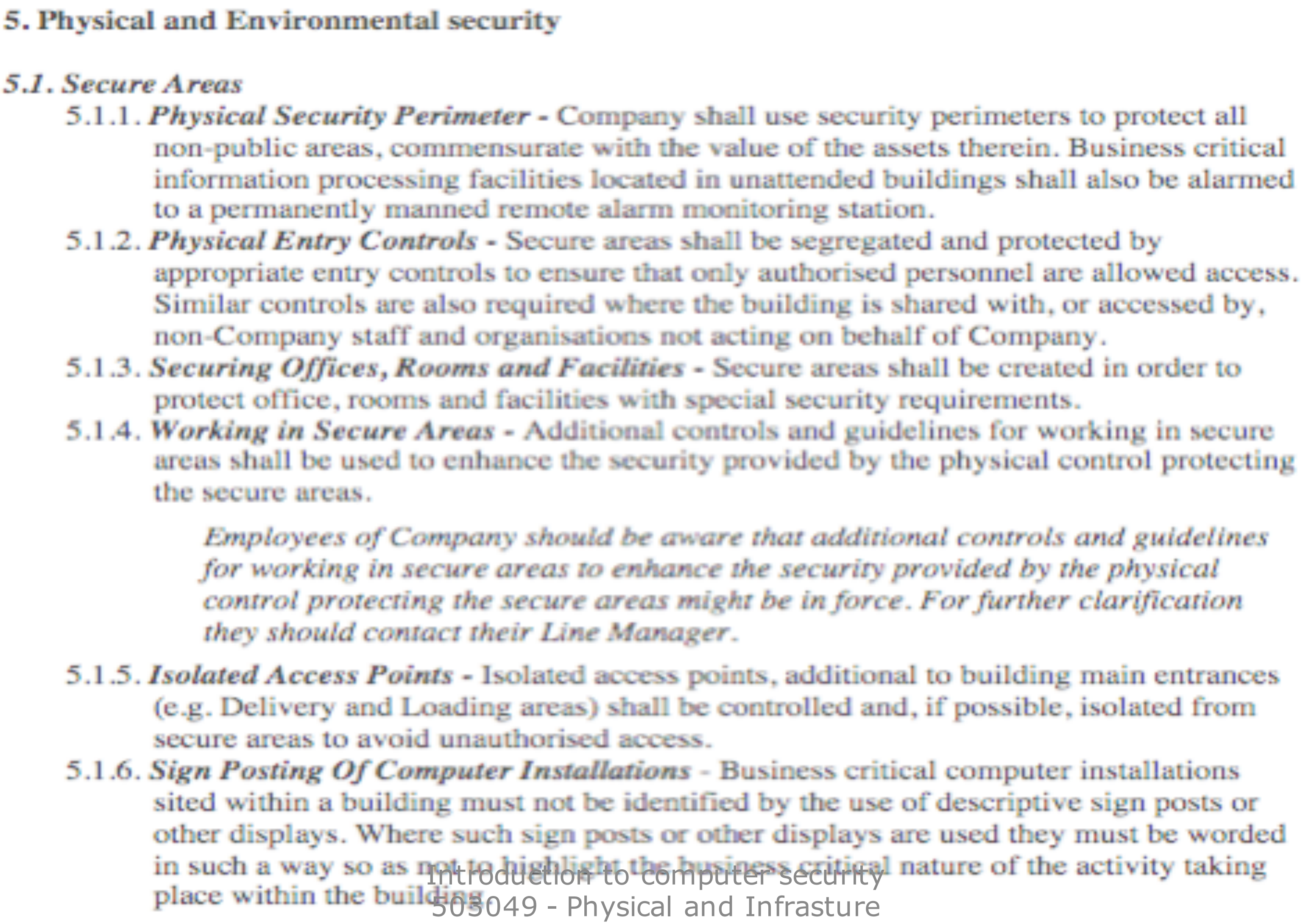
Disaster Recovery: Backup facilities

- Hot sites
  - ready to run
  - readiness at high cost
- Cold sites
  - Building facilities, power, communications
  - No computing resources
- Site sharing
  - Sharing among firms
  - Computing incompatibility
- Need backup tapes/resources at remote site

Threat Assessment

1. Set up a steering committee
2. Obtain information and assistance
3. Identify all possible threats
4. Determine the likelihood of each threat
5. Approximate the direct costs
6. Consider cascading costs
7. Prioritize the threats
8. Complete the threat assessment report

Example Policy



5. Physical and Environmental security

5.1. Secure Areas

5.1.1. ***Physical Security Perimeter*** - Company shall use security perimeters to protect all non-public areas, commensurate with the value of the assets therein. Business critical information processing facilities located in unattended buildings shall also be alarmed to a permanently manned remote alarm monitoring station.

5.1.2. ***Physical Entry Controls*** - Secure areas shall be segregated and protected by appropriate entry controls to ensure that only authorised personnel are allowed access. Similar controls are also required where the building is shared with, or accessed by, non-Company staff and organisations not acting on behalf of Company.

5.1.3. ***Securing Offices, Rooms and Facilities*** - Secure areas shall be created in order to protect office, rooms and facilities with special security requirements.

5.1.4. ***Working in Secure Areas*** - Additional controls and guidelines for working in secure areas shall be used to enhance the security provided by the physical control protecting the secure areas.

Employees of Company should be aware that additional controls and guidelines for working in secure areas to enhance the security provided by the physical control protecting the secure areas might be in force. For further clarification they should contact their Line Manager.

5.1.5. ***Isolated Access Points*** - Isolated access points, additional to building main entrances (e.g. Delivery and Loading areas) shall be controlled and, if possible, isolated from secure areas to avoid unauthorised access.

5.1.6. ***Sign Posting Of Computer Installations*** - Business critical computer installations sited within a building must not be identified by the use of descriptive sign posts or other displays. Where such sign posts or other displays are used they must be worded in such a way so as not to highlight the business critical nature of the activity taking place within the building.

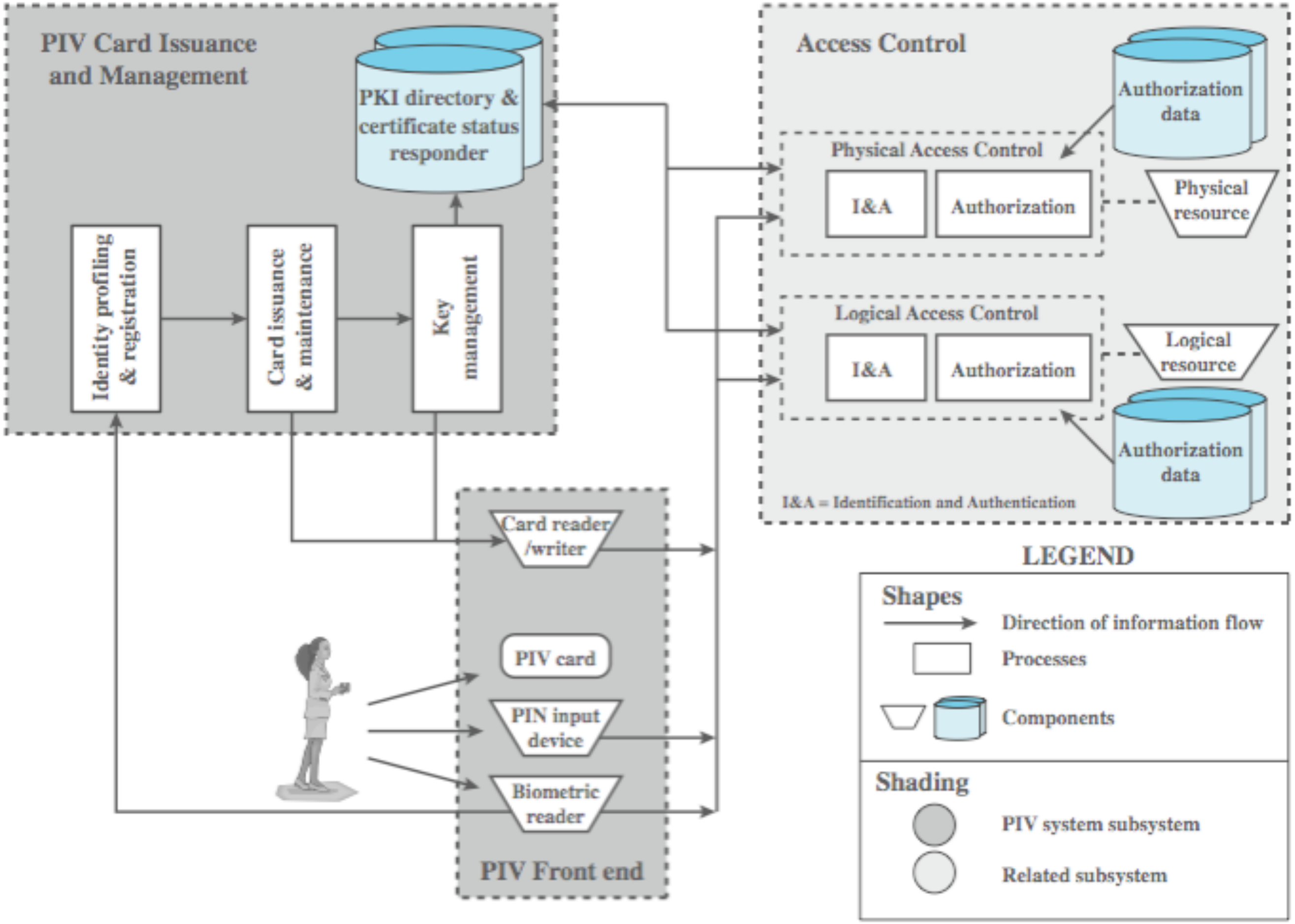
Physical/Logical Security Integration

- Have many detection / prevention devices
- More effective if have central control
- Hence desire to integrate physical and logical security, especially access control
- Need standards in this area
  - FIPS 201-1 “*Personal Identity Verification (PIV) of Federal Employees and Contractors*”

Personal Identity Verification (PIV)

Access control subsystem

Identity proofing



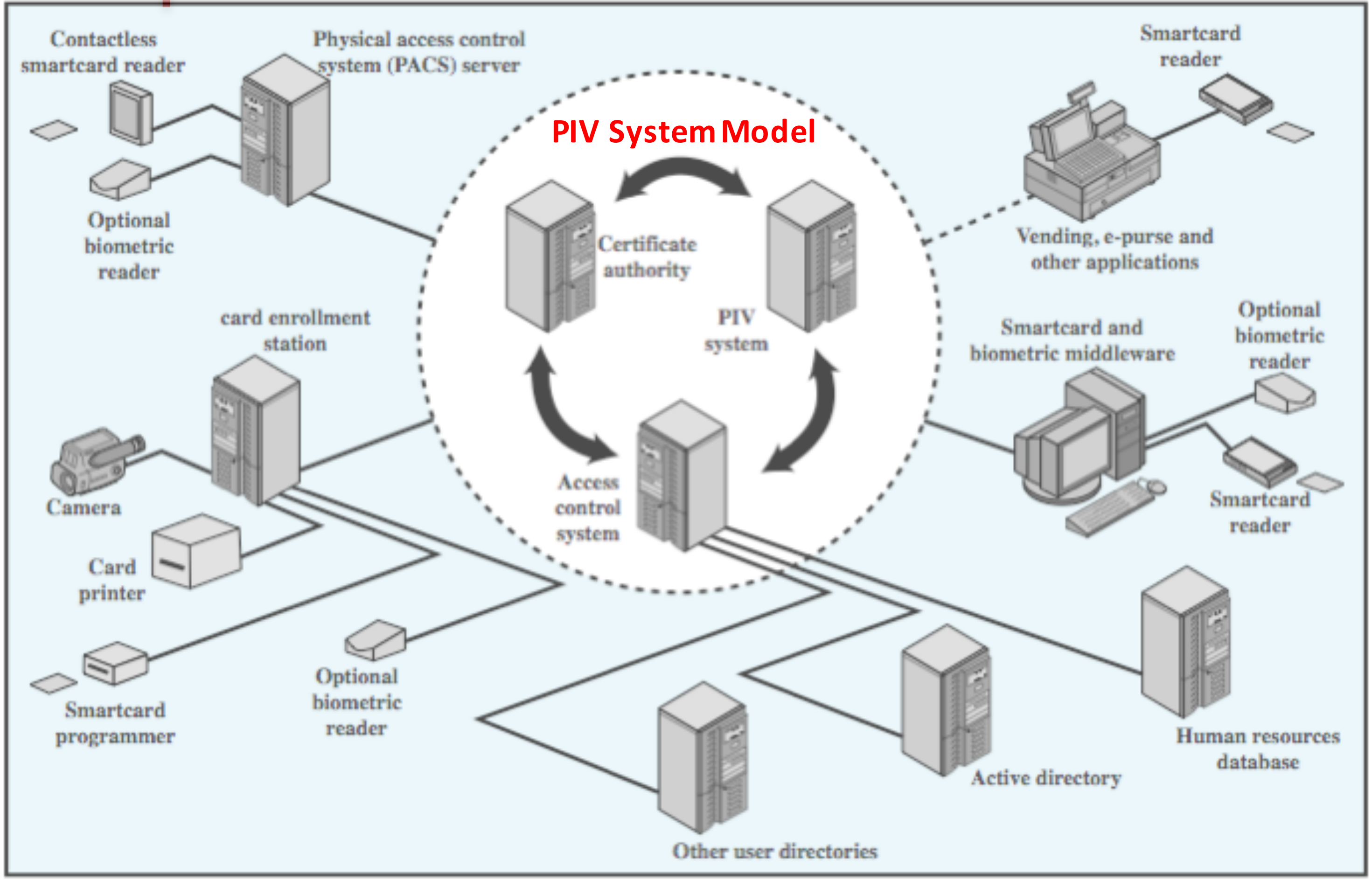
Three assurance levels:

(1) Some confidence (use of smart cards/PIN)

(2) High confidence (plus use of biometrics)

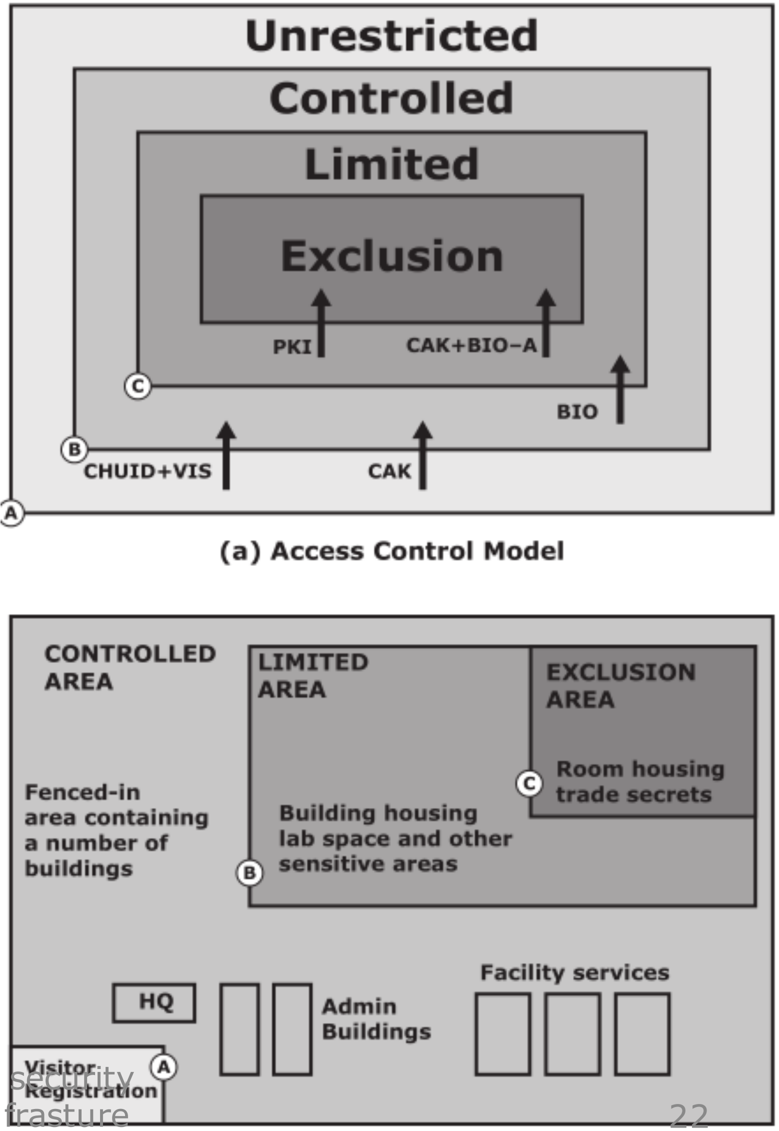
(3) Very high (at the presence of an official observer)

PIV (Physical/Logical) Convergence



FIPS 201 SP 800-116

- Alternative authentication mechanisms that be used for access to a specific area
  - CHUID: card holder unique identification identifier
  - CAK: card authentication key



(a) Access Control Model

(b) Example Use

Summary

- Introduced physical security issues
- Threats: nature, environmental, technical, human
- Mitigation measures and recovery
- Assessment, planning, implementation
- Physical/logical security integration