HARDWARE AND PHYSICAL SECURITY

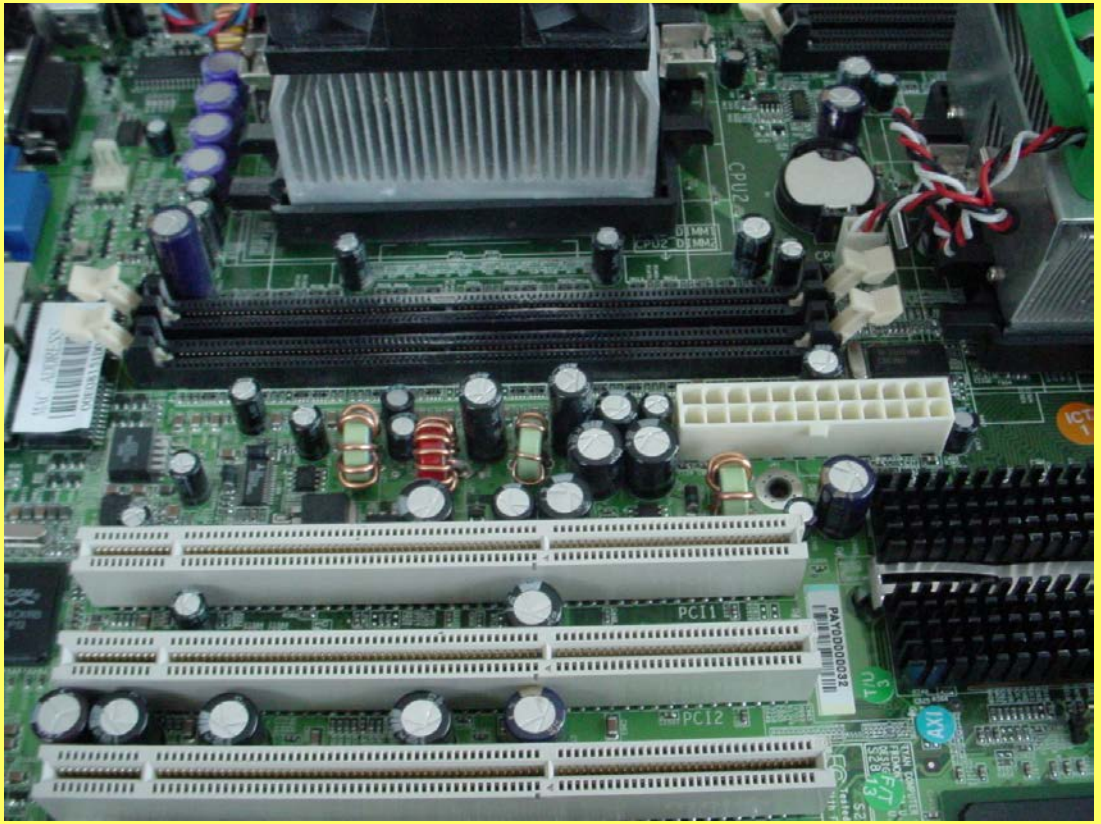
COMPUTER HARDWARE

- **DIFFERENT PARTS INSIDE A COMPUTER**
  - MEMORY
  - MOTHERBOARD
  - SOUND CARD AND VIDEO CARD
  - POWER SUPPLY
  - NETWORK CARD
  - BIOS
  - HARD DISK DRIVE

- **Memory:** When a computer processes information, it uses programs, which requires a certain amount of electronic memory called RAM (Random Access Memory). However, when the computer is turned off, all the information is lost.
- ROM (Read only memory), on the other hand is permanent and it holds the information that was built into it.

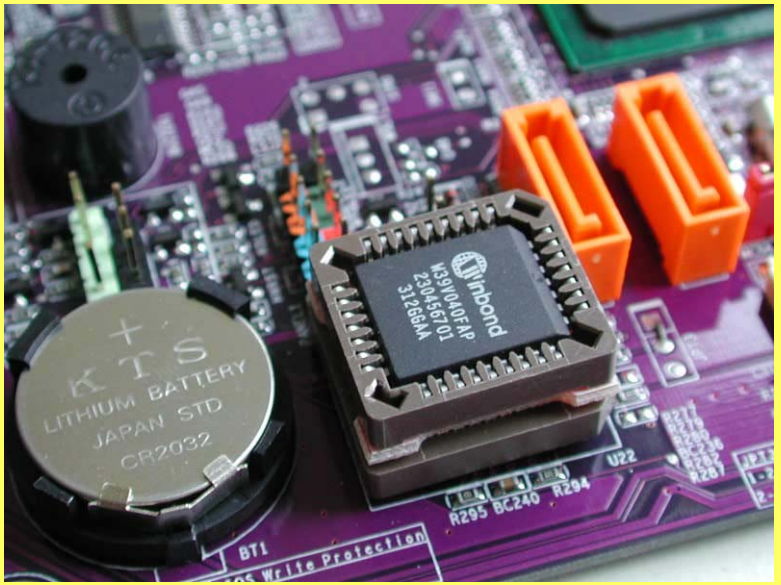
THE MOTHERBOARD

- Each computer has a motherboard, which ties everything together.
- It allows every part of the computer to receive power and communicate with each other.
- Everything that runs the computer or enhances its performance is either part of the motherboard or plugs into one of its expansion slots or ports.



SOUND, VIDEO, BIOS AND NETWORK

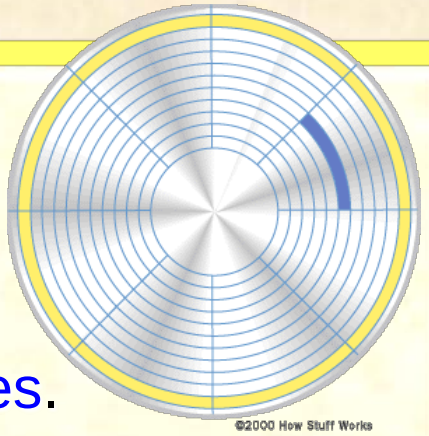
- **Sound and Video Cards**: They contain special circuits that allow computers to play sounds and display graphics on the monitor
- **BIOS Chip:** The Basic Input Output System is a very important computer component; it wakes up the computer when it is tuned on and reminds it what parts it has and what they do.
- **Network card**: It allows computer to be connected to internet.



HARD DISK DRIVE

- The Hard Disk Drive is a magnetic storage device, where computer programs and files you create and save are located there.
- This is permanent storage (at least until you uninstall software or delete a file). The hard drive is normally signified by the drive letter “C”.
- Today’s hard drives can store a HUGE amount of information. A new computer might have a hard drive that will hold 4 Terabytes.
- Hard Disk Drive is a circular disks that is made of steel and has many tracks, or cylinders.
- An electronic reading device called the head passes back and forth over the cylinders, reading information from the disk or writing to it.
- It uses Magnetic Recording Techniques, and it can be easily erased and rewritten.

HARD DISK DRIVE



- **Data in Hard Disk**
- Data is stored on the disk in the form of files.
- A file is simply a named collection of bytes.
- No matter what it contains, a file is simply a string of bytes.
- When a program running on the computer requests a file, the hard disk retrieves its bytes and sends them to the CPU one at a time.
- **Storing the Data**
- Data is stored on the surface of a platter in sectors and tracks.
- Tracks are concentric circles, and sectors are pie-shaped wedges on a track.
- A sector contains a fixed number of bytes -- for example, 256 or 512.
- Either at the drive or the operating system level, sectors are often grouped together into clusters.

HARD DISK DRIVE

- **Removing Unnecessary Files**
- Every time you run a program, install, uninstall, or go on the web, junk files get left behind. It is good to remove these junk files.
- In the System Tools of your computer is a utility called Disk Cleanup.
- **Check the integrity of your hard drive**
- The Windows Operating System includes a utility called Scan Disk.
- Scan Disk is located in the System Tools folder with the Disk Cleanup utility.
- Scan Disk will check the hard drive for errors in the file system and attempt to fix anything it finds.
- **Defragging A Hard Drive**
- As you use your computer, some files can become fragmented, meaning that part of a file may be stored in one location, and the rest of it in another, resulting in slowed performance.
- It makes sense that if the computer only had to look in one location to get an entire file, it would perform faster. Defragging a hard drive will accomplish this.

SS DRIVE

- An SSD (Solid State Drive) performs the same basic function as a hard drive, but data is instead stored on interconnected flash-memory chips that retain the data even when there's no power flowing through them.
- The flash chips are also used in USB thumb drives, however the ones used in SSD are faster, more reliable and more expensive than USB thumb drives of the same capacities.
- SSDs are often much smaller than HDDs and therefore offer manufacturers more flexibility in designing a PC.
- While they can take the place of traditional 2.5-inch or 3.5-inch hard drive bays, they can also be installed in a PCI Express expansion slot or even be mounted directly on the motherboard.

SSD

- HDD technology is relatively ancient, while the SSD has a much shorter history, though its roots do reach several decades into the past (1970 and 80, but then died away).
- The first primary drives that we know as SSDs started appearing during the rise of netbooks in the late 2000s.
- HDD are still around in budget and older systems, but SSDs are now the rule in mainstream systems.
- Both do the same job, e.g., boot computer, store applications and personal files, however, each has its own unique qualities.
- An SSD-equipped PC will boot in less than a minute (often in seconds), while HDD will require more time.
- An SSD has no moving parts, so it is more likely to keep your data safe in the event you drop your laptop.
- Even the quietest HDD will emit a bit of noise when it is in use, while SSDs make no noise at all; they're non-mechanical.

HOW FILES ARE CREATED, DELETED, AND RESTORED

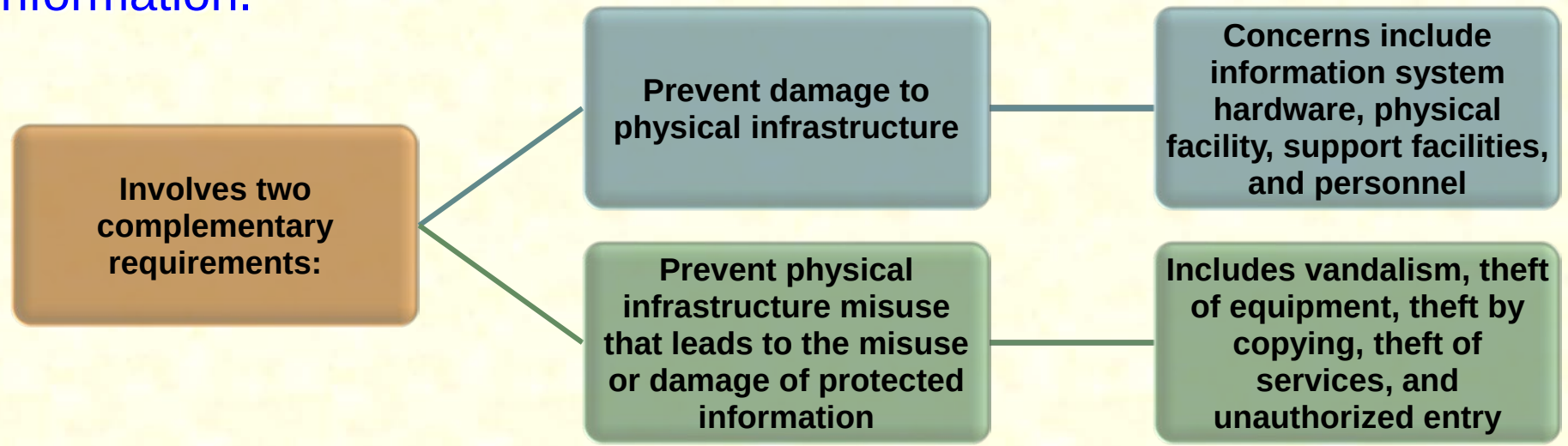
- **File Creation**
- When a file is created three things occur:
  1. An entry is made into the File Allocation Table (FAT) to indicate where the actual data is stored in the Data Area.
  2. A Directory entry is made to indicate file name, size, the link to the FAT and other info.
  3. The data is written to the Data Area.
- **File Deletion**
- When a file is deleted only two things occur:
  1. The FAT entry for the file is zeroed out and the space on the hard drive becomes available for use by a new file.
  2. The first character of the Directory entry file name is changed to a special character.
- Nothing is done to the Data Area.

HOW FILES ARE CREATED, DELETED, AND RESTORED

- **File Restoration**
- When a file is restored only two things are done:
  1. The FAT entry for the file is linked again to the location in the data area where the file is stored.
  2. The first character of the Directory entry file name is changed to a legal character.
- Nothing is done to the Data Area.
- Before you dispose of your old computer or any digital device which has secondary storage, it is important to make sure your computer's hard drive is completely free of data.
- Physically smash the hard drive is not good enough.
- Formatting a disk does not erase the data on the disk, only the address tables and therefore it is not 100% secure.
- You need disk wiping (or disk sanitizing) or overwriting with random bits.

PHYSICAL SECURITY

- Physical security is 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 security.
- Protect physical assets that support the storage and processing of information.



PHYSICAL SECURITY

- For information systems, the role of physical security is to protect the physical assets that support the storage and processing of information.
- Physical security involves two complementary requirements.
- **First**, physical security must prevent damage to the physical infrastructure that sustains the information system. In broad terms, that infrastructure includes the following:
- **Information system hardware:** Includes data processing and storage equipment, transmission and networking facilities, and offline storage media.
- **Physical facility**: The buildings and other structures housing the system and network components.
- **Supporting facilities**: This category includes electrical power, communication services, and environmental controls (heat, humidity, etc.).
- **Personnel:** Humans involved in the control, maintenance, and use of the information systems.
- **Second,** physical security must prevent misuse of the physical infrastructure, which includes vandalism, theft, and unauthorized entry.

PHYSICAL SECURITY THREATS

Physical situations and occurrences that threaten information systems

- Environmental threats
- Technical threats
- Human-caused threats

PHYSICAL SECURITY THREATS

- It refers to the types of physical situations and occurrences that can constitute a threat to information systems.
- It is important to understand the spectrum of threats to information systems so that responsible administrators can ensure that prevention measures are comprehensive.
- Physical threats can be categorized into the following categories:
  1. Environmental threats
  2. Technical threats
  3. Human-caused threats
- Even though natural disasters are prime source of environmental threat, it is not the only, source of environmental threats.
- The technical and human-caused threats are also important when it comes to physical protection of devices and networks.

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

CHARACTERISTICS OF NATURAL DISASTERS

- Natural disasters are the source of a wide range of environmental threats to data centers, other information processing facilities, and their personnel.
- A tornado can generate winds that exceed hurricane strength in a narrow band along the tornado's path. There is substantial potential for structural damage, roof damage, and may be damage from wind and flying debris.
- Hurricanes, tropical storms, and typhoons, collectively known as tropical cyclones, are among the most devastating naturally occurring hazards. Depending on strength, cyclones may also cause significant structural damage and damage to outside equipment at a particular site.
- A major earthquake has the potential for the greatest damage and occurs without warning. A facility near the epicenter may suffer catastrophic, even complete, destruction, with significant and long-lasting damage to data centers and other IS facilities.
- An ice storm or blizzard can cause some disruption of or damage to IS facilities.
- The consequences of lightning strikes can range from no impact to disaster.
- Flood is a concern in areas that are subject to flooding and damage can be severe, with long-lasting effects and the need for a major cleanup operation.

WATER DAMAGE

Water and other stored liquids in proximity to computer equipment pose an obvious threat.

Primary danger is an electrical short

A pipe may burst from a fault in the line or from freezing

Sprinkler systems set off accidentally

Floodwater leaving a muddy residue and suspended material in the water

Due diligence should be performed to ensure that water from as far as two floors above will not create a hazard

CHEMICAL, RADIOLOGICAL, AND BIOLOGICAL HAZARDS

- Chemical, radiological, and biological hazards pose a growing threat, both from intentional attack and from accidental discharge.
- None of these hazardous agents should be present in an information system environment, but either accidental or intentional intrusion is possible.
- Nearby discharges (e.g., from an overturned truck carrying hazardous materials) can be introduced through the ventilation system or open windows and, in the case of radiation, through perimeter walls.
- In addition, discharges in the vicinity can disrupt work by causing evacuations to be ordered.
- Flooding can also introduce biological or chemical contaminants.
- In general, the primary risk of these hazards is to personnel. Radiation and chemical agents can also cause damage to electronic equipment.

DUST AND INFESTATION

Dust

- Often overlooked
- Rotating storage media and computer fans are the most vulnerable to damage.
- Can also block ventilation
- Influxes can result from a number of things:
  - Controlled explosion of a nearby building
  - Windstorm carrying debris
  - Construction or maintenance work in the building

Infestation

- Covers a broad range of living organisms:
  - High-humidity conditions can cause mold and mildew.
  - Insects, particularly those that attack wood and paper.

TECHNICAL THREATS

- Electrical power is essential to run equipment, however it can cause problems that can be broadly grouped into three categories: undervoltage, overvoltage, and noise.
- **Under-voltage**: This condition occurs when the IS equipment receives less voltage than is required for normal operation. Undervoltage events range from temporary dips in the voltage supply, to brownouts (prolonged undervoltage), to power outages. Most computers are designed to withstand prolonged voltage reductions of about 20% without shutting down and without operational error.
- **Over-voltage:** Far more serious is an overvoltage condition. A surge of voltage can destroy silicon-based components, including processors and memories.

Electromagnetic interference (EMI)

- Noise along a power supply line, motors, fans, heavy equipment, other computers, cell phones, microwave relay antennas, nearby radio stations
- Noise can be transmitted through space as well as through power lines
- Can cause intermittent problems with computers

HUMAN-CAUSED THREATS

- **Unauthorized physical access:** Those without the proper authorization should not be allowed access to certain portions of a building or complex unless accompanied with an authorized individual.
  - Information assets such as servers, mainframe computers, network equipment, and storage networks are generally located in a restricted area, with access limited to a small number of employees. Unauthorized physical access can lead to other threats, such as theft, vandalism, or misuse.
- **Theft:** This threat includes theft of equipment and theft of data by copying. Eavesdropping and wiretapping also fall into this category. Theft can be at the hands of an outsider who has gained unauthorized access or by an insider.
- **Vandalism**: This threat includes destruction of equipment and data.
- **Misuse**: This category includes improper use of resources by those who are authorized to use them, as well as use of resources by individuals not authorized.

PHYSICAL ACCESS CONTROLS

- **Secure facility:** physical location with controls implemented to minimize the risk of attacks from physical threats.
- Secure facility can take advantage of natural terrain, local traffic flow, and surrounding development and can complement these with protection mechanisms (fences, gates, walls, guards, alarms).
- **Physical Security Controls**
  - Walls, fencing, and gates
  - Guards
  - Dogs
  - ID cards and badges
  - Locks and keys
  - Mantraps
  - Electronic monitoring
  - Alarms and alarm systems
  - Computer rooms and wiring closets
  - Interior walls and doors

PHYSICAL ACCESS CONTROLS

- **Walls, Fencing, and Gates**
  - Some of the oldest and most reliable elements of physical security; the essential starting point for perimeter control.
- **Guards**
  - Can evaluate each situation as it arises to make reasoned responses; most have standard operating procedures.
- **Dogs**
  - Keen sense of smell and hearing can detect intrusions that human guards cannot.
- **ID Cards and Badges**
  - ID card is typically concealed, and name badge is visible.
  - Serve as a simple form of biometrics (facial recognition)
  - Should not be the only means of control as cards can be easily duplicated, stolen, and modified.
  - Tailgating occurs when an authorized individual opens a door and other people also enter.

Tailgating

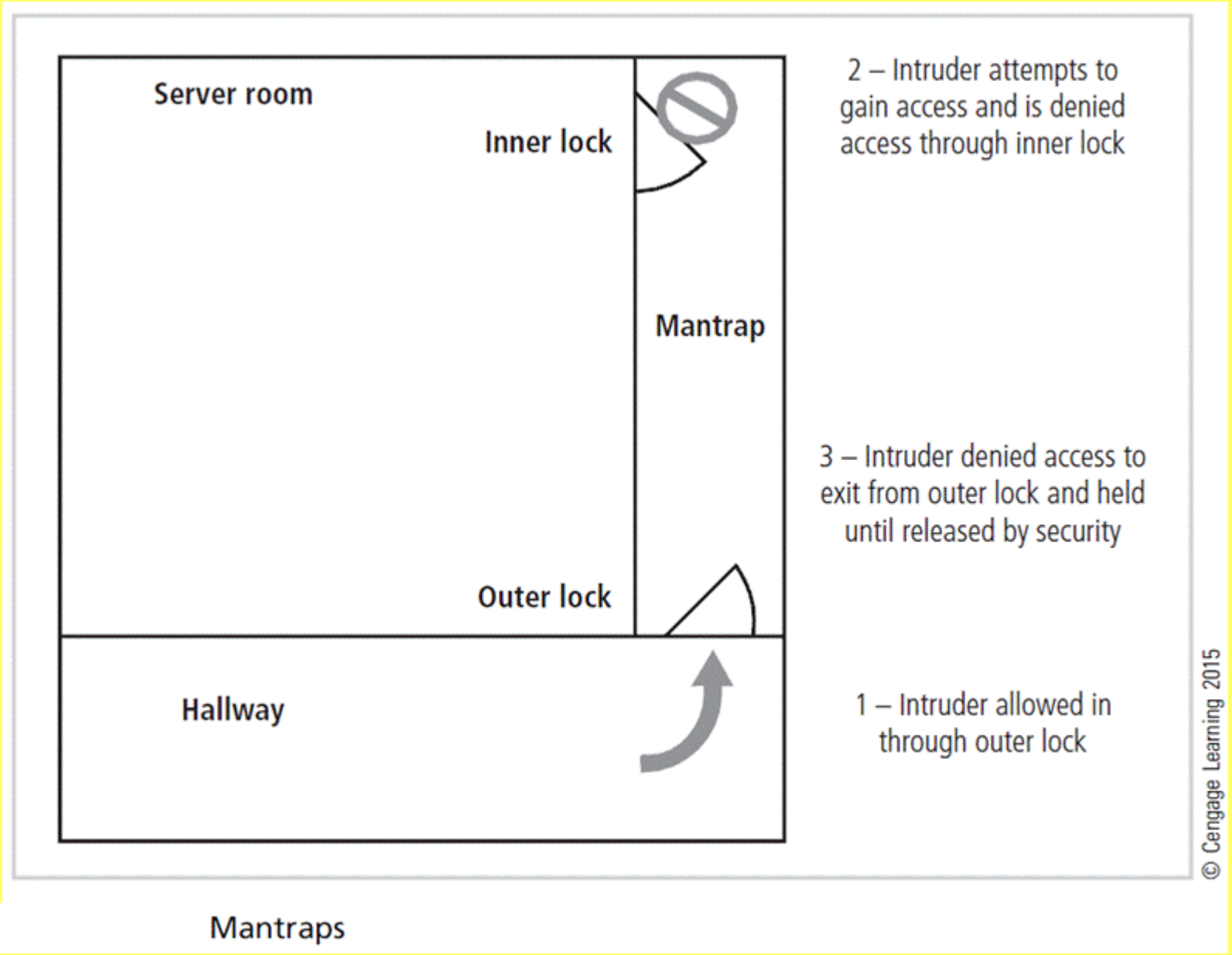
PHYSICAL ACCESS CONTROLS

- **Locks and keys**
  - Two types of locks: mechanical and electronics
  - Locks can also be divided into four categories: manual, programmable, electronic, biometric.
  - Locks fail and alternative procedures for controlling access must be put in place.
- **Mantraps**
  - Small enclosure that has an entry point and a different exit point.
  - Individual enters mantrap, requests access, and, if verified, is allowed to exit mantrap into facility.
  - Individual denied entry is not allowed to exit until the security official overrides automatic locks of the enclosure.

Programmable/mechanical

Electronic

Locks


Server room
Inner lock
Mantrap
Outer lock
Hallway
2 – Intruder attempts to gain access and is denied access through inner lock
3 – Intruder denied access to exit from outer lock and held until released by security
1 – Intruder allowed in through outer lock
© Cengage Learning 2015

Mantraps

PHYSICAL ACCESS CONTROLS

- **Electronic Monitoring**
  - Equipment can record events in areas where other types of physical controls are impractical.
  - May use cameras with video recorders; includes closed-circuit television (CCT) systems.
- **Drawbacks**
  - Passive; does not prevent access or prohibited activity.
  - Recordings often are not monitored in real time; must be reviewed to have any value.
- **Alarms and alarm systems**
  - Alarm systems notify people/systems when an event occurs.
  - Detect fire, intrusion, environmental disturbance, or an interruption in services.
  - Rely on sensors that detect an event, for example, motion detectors, thermal detectors, glass breakage detectors, weight sensors, and contact sensors.

PHYSICAL ACCESS CONTROLS

- **Computer rooms and wiring closets**
  - Require special attention to ensure confidentiality, integrity, and availability of information.
  - Logical access controls are easily defeated if attacker gains physical access to computing equipment.
  - Custodial staff, often the least scrutinized people who have access to offices, are given greatest degree of unsupervised access.
- **Interior walls and doors**
  - Information asset security is sometimes compromised by improper construction of facility walls and doors.
  - Facility walls are typically either standard interior or firewall.
  - High-security areas must have firewall-grade walls to provide physical security against potential intruders and fires.
  - Doors allowing access to high-security rooms should be evaluated.
  - To secure doors, install push or crash bars on computer rooms and closets.

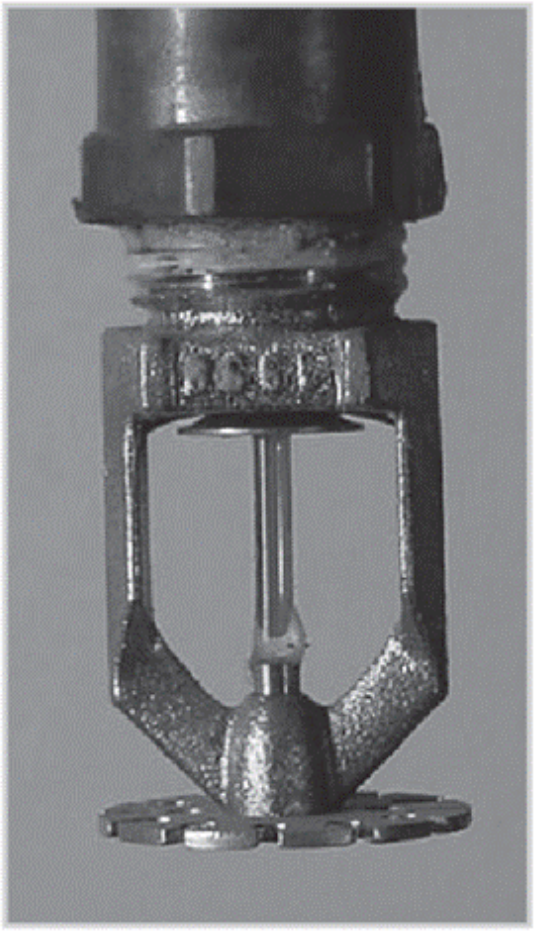
FIRE SECURITY AND SAFETY

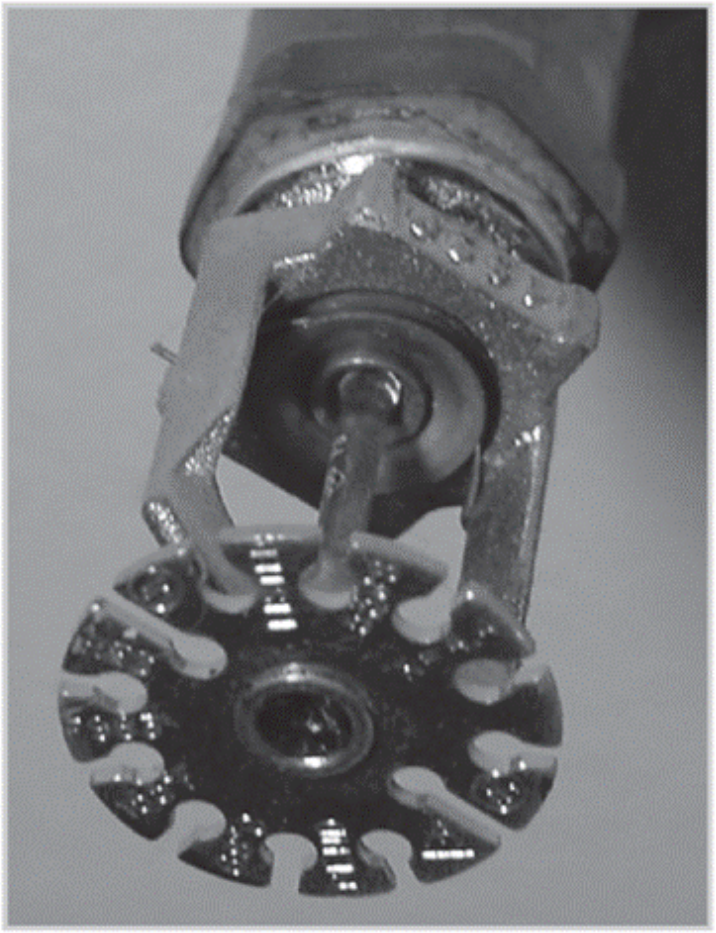
- Most serious threat to safety of people who work in an organization is fire.
- Fires account for more property damage, personal injury, and death than any other threat.
- It is imperative that physical security plans implement strong measures to detect and respond to fires and fire hazards.
- **Fire Detection and Response**
  - **Fire suppression systems**: devices installed and maintained to detect and respond to a fire, potential fire, or combustion danger
  - Flame point: temperature of ignition
  - Deny an environment of temperature, fuel, or oxygen
  - Water and water mist systems
  - Carbon dioxide systems
  - Soda acid systems
  - Gas-based systems

FIRE DETECTION AND RESPONSE

- **Fire detection**
  - Fire detection systems fall into two general categories: manual and automatic
  - To prevent an attacker slipping into offices during an evacuation, programs often designate a person from each office area to serve as a floor monitor.
  - There are three basic types of fire detection systems: thermal detection, smoke detection, flame detection.
- **Fire suppression**
  - Systems can consist of portable, manual, or automatic apparatus.
  - Portable extinguishers are rated by the type of fire: Class A, Class B, Class C, Class D, Class K.
  - Installed systems apply suppressive agents, usually either sprinkler or gaseous systems.

A		Ordinary Combustibles	Wood, Paper, Cloth, Etc.
B		Flammable Liquids	Grease, Oil, Paint, Solvents
C		Live Electrical Equipment	Electrical Panel, Motor, Wiring, Etc.
D		Combustible Metal	Magnesium, Aluminum, Etc.
K		Commercial Cooking Equipment	Cooking Oils, Animal Fats, Vegetable Oils





When the ambient temperature reaches 140–150° F, the liquid-filled glass tube trigger breaks, releasing the stopper and allowing water to hit the diffuser, spraying water throughout the area

Water sprinkler system

HEATING, VENTILATION, AND AIR CONDITIONING

- Areas within heating, ventilation, and air conditioning (HVAC) systems that can cause damage to information systems include:
- Temperature
- Filtration
- Humidity
- Static electricity

Voltage	Possible damage
40	High probability of damage to sensitive circuits and transistors
1,000	Scrambles monitor display
1,500	Can cause disk drive data loss
2,000	High probability of system shutdown
4,000	May jam printers
17,000	Causes certain and permanent damage to almost all microcircuitry

Static Charge Damage in Computers[8]

HEATING, VENTILATION, AND AIR CONDITIONING

- **Ventilation shafts**
  - While ductwork is small in residential buildings, in large commercial buildings it can be large enough for an individual to climb through.
  - If ducts are large, security can install wire mesh grids at various points to compartmentalize the runs.
- **Power management and conditioning**
  - Power systems used by information-processing equipment must be properly installed and correctly grounded.
  - Noise that interferes with the normal 60 Hertz cycle can result in inaccurate time clocks or unreliable internal clocks inside CPU.
- **Grounding**
  - Grounding ensures that returning flow of current is properly discharged to ground.
  - Overloading a circuit can create a load exceeding electrical cable's rating, increasing the risk of overheating and fire.

HEATING, VENTILATION, AND AIR CONDITIONING

- **Uninterruptible power supply (UPS)**
  - In case of power outage, UPS is the backup power source for major computing systems.
  - **Basic UPS configurations**:
    - Standby
    - Line-interactive
    - Standby online hybrid
    - Double conversion online
    - Data conversion online
    - Emergency shutoff
      - Important aspect of power management is the ability to stop power immediately if the current represents a risk to human or machine safety.
      - Most computer rooms and wiring closets are equipped with an emergency power shutoff.

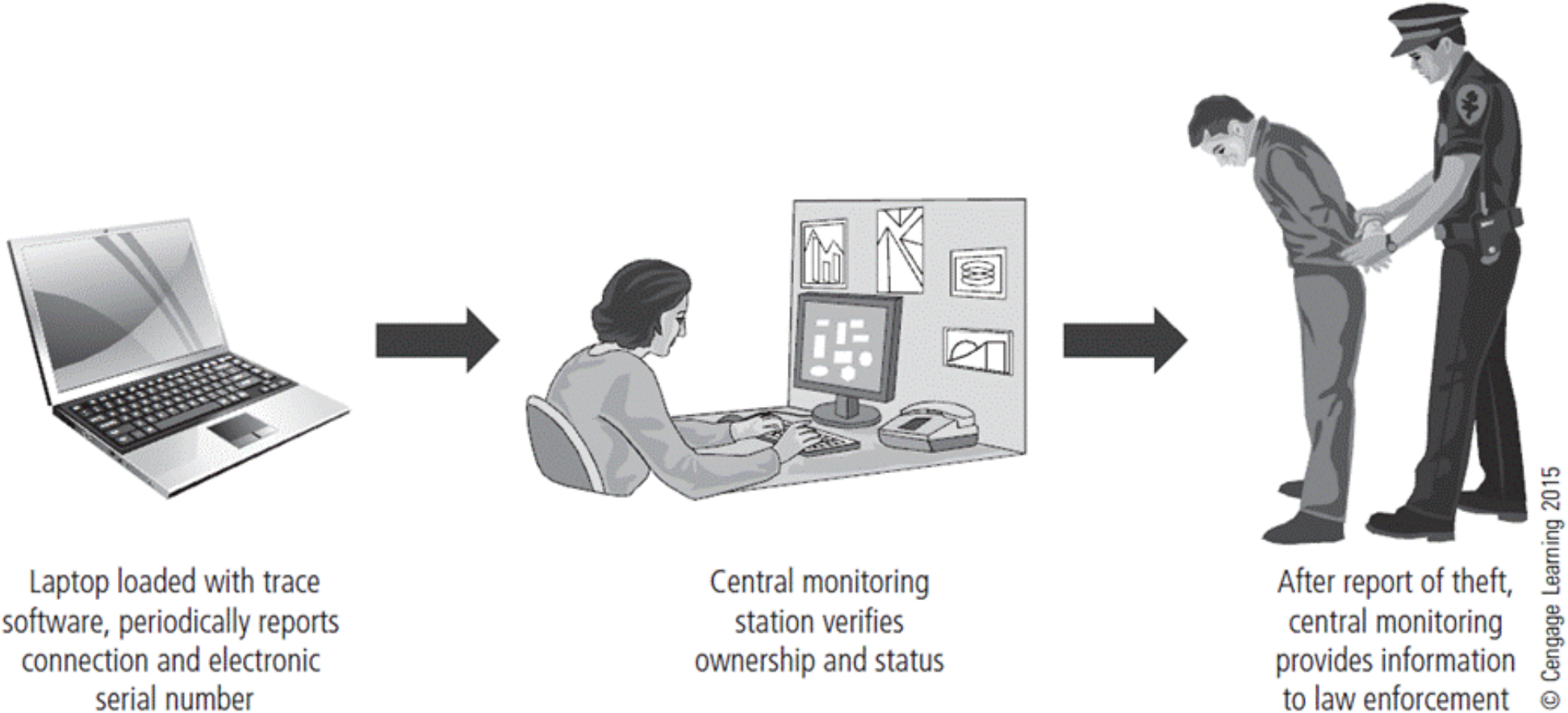
OTHER DETECTION AND PROTECTIONS

- **Water Problems**
  - Lack of water poses problem to systems, including fire suppression and air-conditioning systems.
  - Surplus of water, or water pressure, poses a real threat (flooding, leaks).
  - Very important to integrate water detection systems into alarm systems that regulate overall facility operations
- **Structural Collapse**
  - Unavoidable environmental factors/forces can cause failures in structures that house an 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.

SECURING MOBILE AND PORTABLE SYSTEMS

- Mobile computing requires more security than typical computing infrastructures on the organization's premises.
- Many mobile computing systems have corporate information stored within them.
- Some are configured to facilitate user's access into organization's secure computing facilities.
- Controls support security and retrieval of lost or stolen laptops .
- CompuTrace software, stored on laptop; reports to a central monitoring center.
- Burglar alarms are made up of a PC card that contains a motion detector.

SECURING MOBILE AND PORTABLE SYSTEMS



Laptop theft deterrence

CONSIDERATIONS FOR PHYSICAL SECURITY THREATS

- Develop physical security in-house or outsource?
- There are 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.
- **Social engineering**: Should train staff so that they don't release information via social engineering attacks.
- **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.

SUMMARY

- Threats to information security are unique to physical security.
- Each facility must make it as a Key physical security considerations.
- There are many physical security monitoring components.
- Each facility must have essential elements of access control in place.
- Fire safety, fire detection, and response must be implemented.
- Importance of supporting utilities, especially use of uninterruptible power supplies is very important.
- Countermeasures to physical theft of computing devices must be in place.