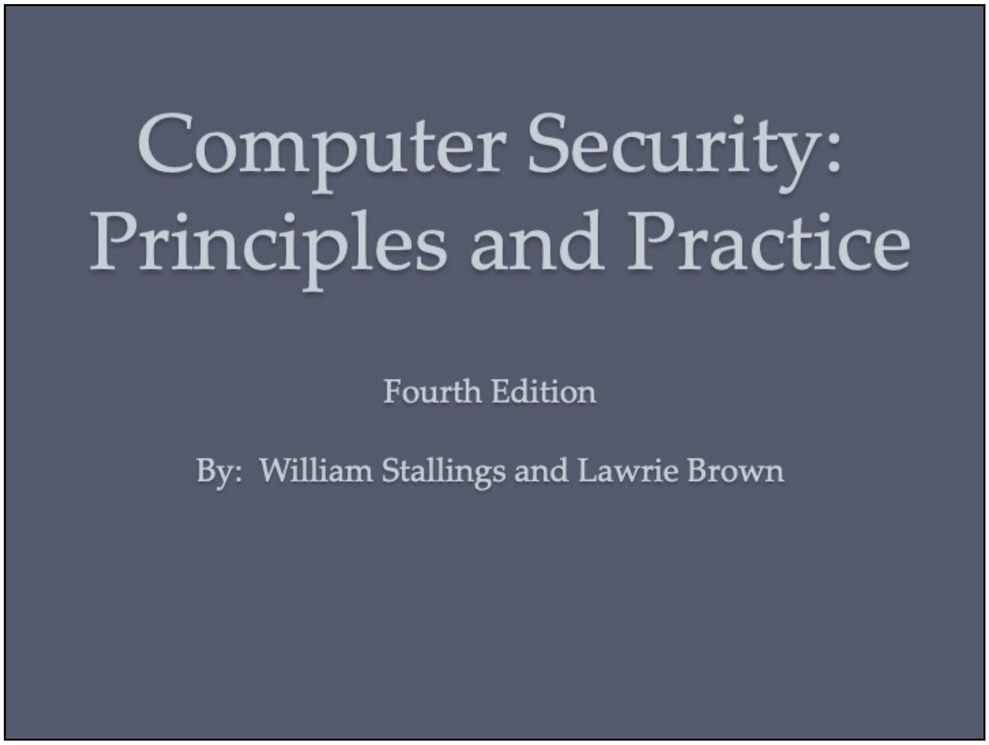
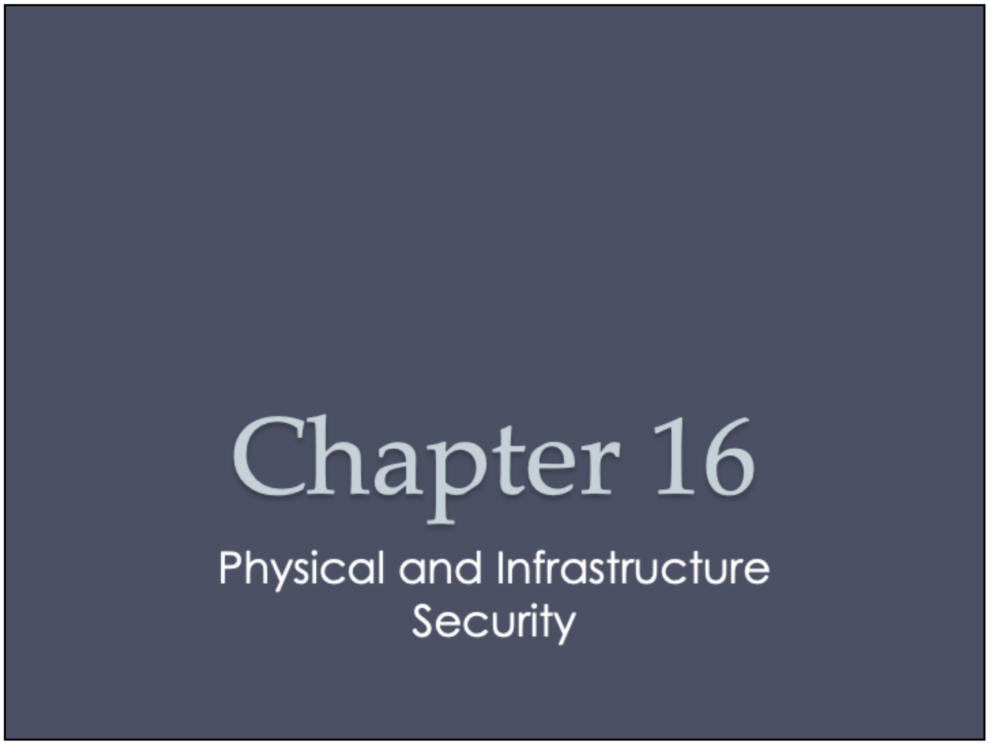


Computer Security: Principles and Practice

Fourth Edition

By: William Stallings and Lawrie Brown

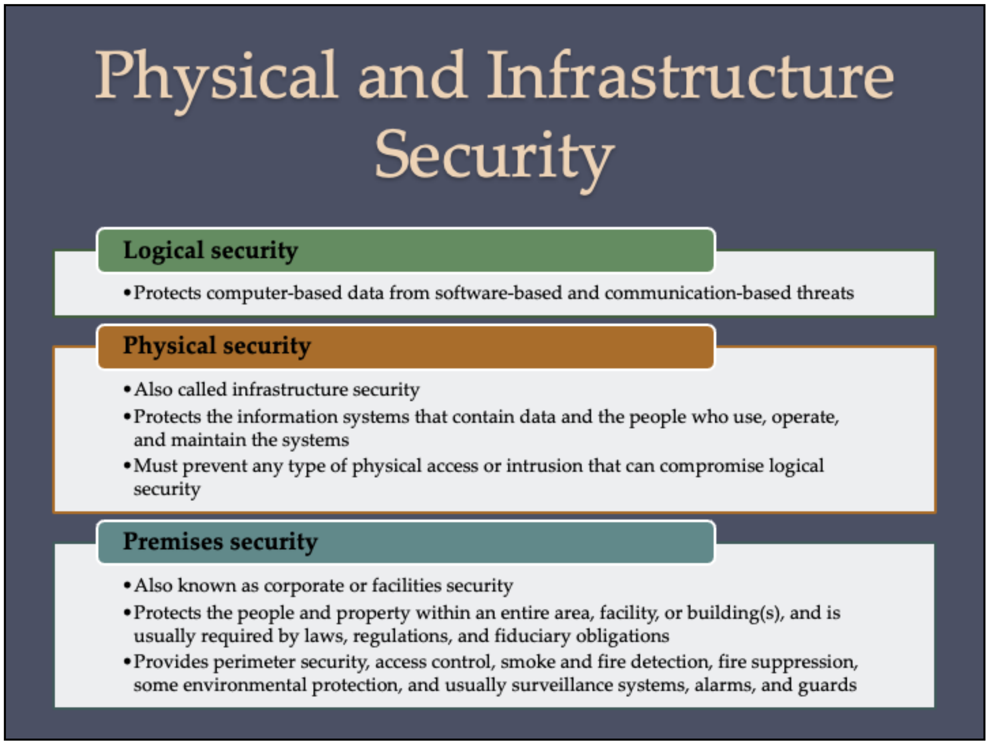
Lecture slides prepared for “Computer Security: Principles and Practice”, 4/e, by William Stallings and Lawrie Brown, Chapter 16, “Physical and Infrastructure Security”.



Chapter 16

Physical and Infrastructure Security

This chapter is concerned with physical security and with some overlapping areas of premises security. We survey a number of threats to physical security and a number of approaches to prevention, mitigation, and recovery. To implement a physical security program, an organization must conduct a risk assessment to determine the amount of resources to devote to physical security and the allocation of those resources against the various threats. This process also applies to logical security. This assessment and planning process is covered in Chapters 14 and 15 .



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

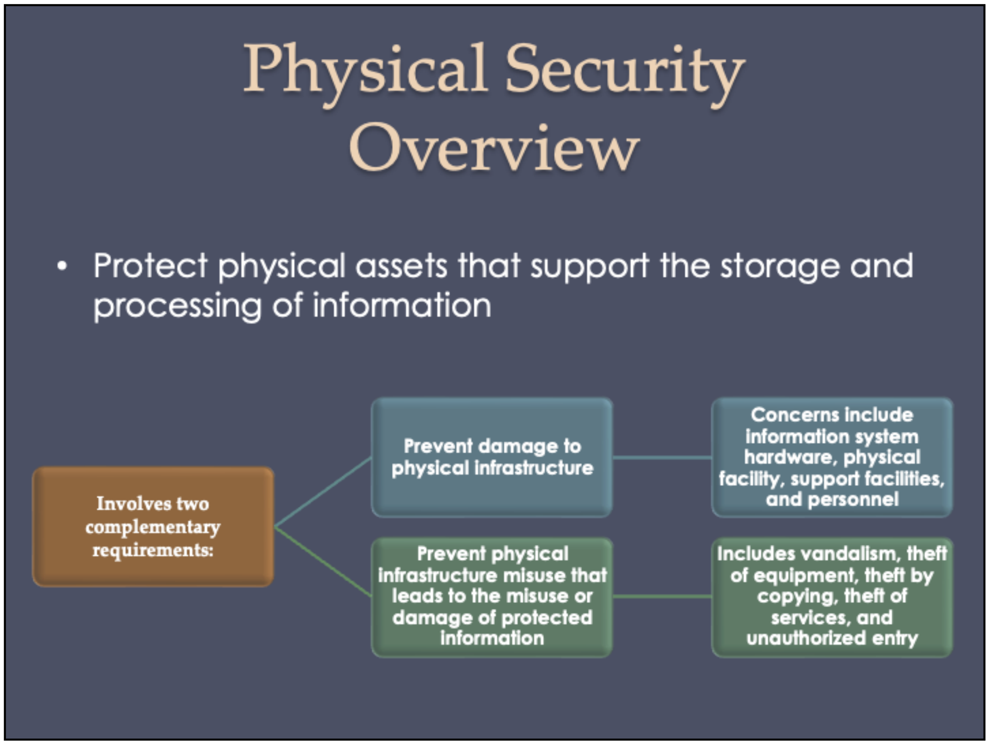
- Also known as corporate or facilities security
- Protects the people and property within an entire area, facility, or building(s), and is usually required by laws, regulations, and fiduciary obligations
- Provides perimeter security, access control, smoke and fire detection, fire suppression, some environmental protection, and usually surveillance systems, alarms, and guards

[PLAT14] distinguishes three elements of information system (IS) security:

• **Logical security**: Protects computer-based data from software-based and communication-based threats. The bulk of this book deals with logical security.

• **Physical security**: Also called **infrastructure security** . Protects the information systems that contain data and the people who use, operate, and maintain the systems. Physical security also 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. Premises security provides perimeter security, access control, smoke and fire detection, fire suppression, some environmental protection, and usually surveillance systems, alarms, and guards.



Physical Security Overview

- Protect physical assets that support the storage and processing of information

Involves two complementary requirements:

Prevent damage to physical infrastructure

Concerns include information system hardware, physical facility, support facilities, and personnel

Prevent physical infrastructure misuse that leads to the misuse or damage of protected information

Includes vandalism, theft of equipment, theft by copying, theft of services, and unauthorized entry

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:

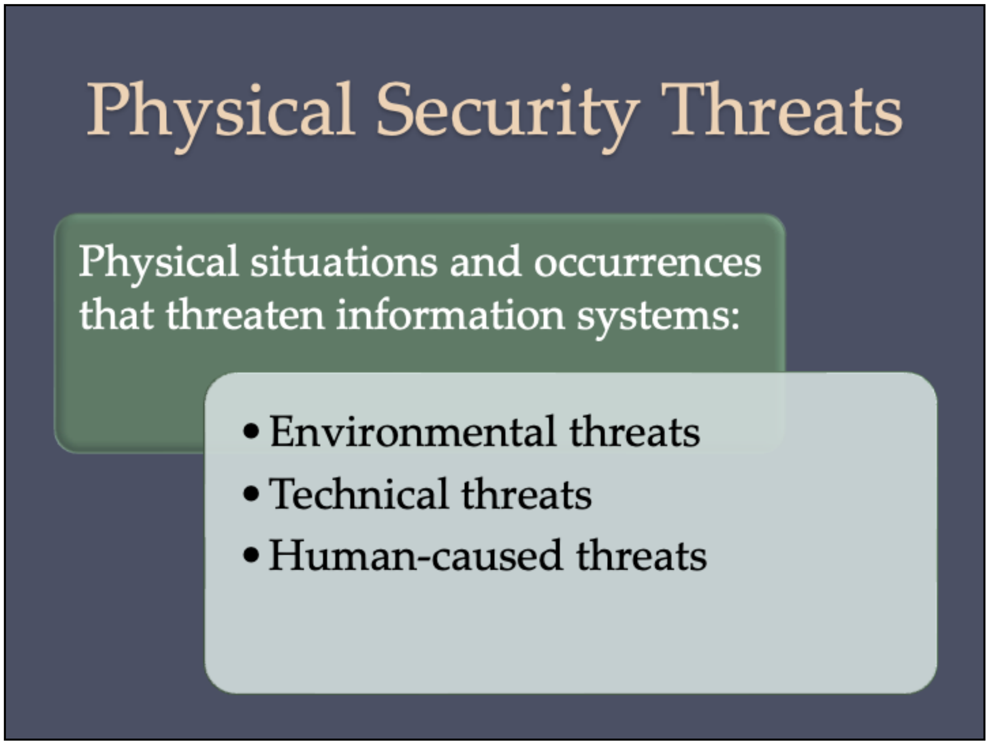
• **Information system hardware**: Includes data processing and storage equipment, transmission and networking facilities, and offline storage media. We can include in this category supporting documentation.

• **Physical facility**: The buildings and other structures housing the system and network components.

• **Supporting facilities**: These facilities underpin the operation of the information system. 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 that leads to the misuse or damage of the protected information. The misuse of the physical infrastructure can be accidental or malicious. It includes vandalism, theft of equipment, theft by copying, theft of services, and unauthorized entry.



Physical Security Threats

Physical situations and occurrences that threaten information systems:

- Environmental threats
- Technical threats
- Human-caused threats

In this section, we look at the types of physical situations and occurrences that can constitute a threat to information systems. There are a number of ways in which such threats can be categorized. It is important to understand the spectrum of threats to information systems so that responsible administrators can ensure that prevention measures are comprehensive. We organize the threats into the following categories:

• Environmental threats

• Technical threats

• Human-caused threats

We begin with a discussion of natural disasters, which are a prime, but not the only, source of environmental threats. Then we look specifically at environmental threats, followed by technical and human-caused threats.

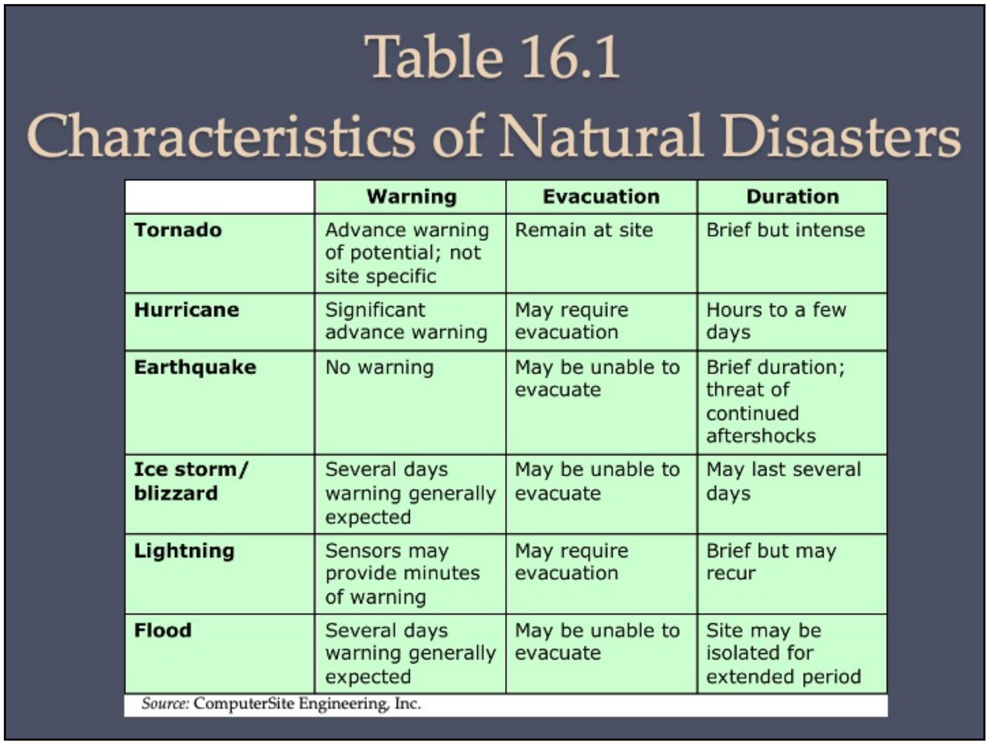


Table 16.1
Characteristics of Natural Disasters

	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.

Natural disasters are the source of a wide range of environmental threats to data centers, other information processing facilities, and their personnel. It is possible to assess the risk of various types of natural disasters and take suitable precautions so that catastrophic loss from natural disaster is prevented.

Table 16.1 lists six categories of natural disasters, the typical warning time for each event, whether or not personnel evacuation is indicated or possible, and the typical duration of each event. We comment briefly on the potential consequences of each type of disaster.

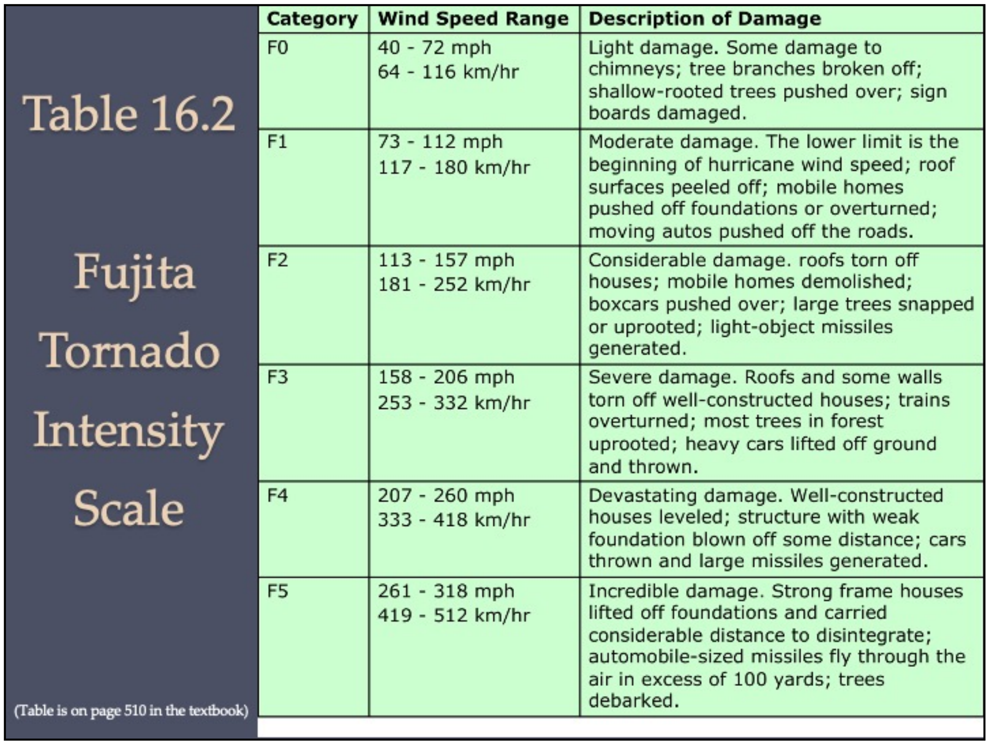


Table 16.2

Fujita Tornado Intensity Scale

Category	Wind Speed Range	Description of Damage
F0	40 - 72 mph 64 - 116 km/hr	Light damage. Some damage to chimneys; tree branches broken off; shallow-rooted trees pushed over; sign boards damaged.
F1	73 - 112 mph 117 - 180 km/hr	Moderate damage. The lower limit is the beginning of hurricane wind speed; roof surfaces peeled off; mobile homes pushed off foundations or overturned; moving autos pushed off the roads.
F2	113 - 157 mph 181 - 252 km/hr	Considerable damage. roofs torn off houses; mobile homes demolished; boxcars pushed over; large trees snapped or uprooted; light-object missiles generated.
F3	158 - 206 mph 253 - 332 km/hr	Severe damage. Roofs and some walls torn off well-constructed houses; trains overturned; most trees in forest uprooted; heavy cars lifted off ground and thrown.
F4	207 - 260 mph 333 - 418 km/hr	Devastating damage. Well-constructed houses leveled; structure with weak foundation blown off some distance; cars thrown and large missiles generated.
F5	261 - 318 mph 419 - 512 km/hr	Incredible damage. Strong frame houses lifted off foundations and carried considerable distance to disintegrate; automobile-sized missiles fly through the air in excess of 100 yards; trees debarked.

(Table is on page 510 in the textbook)

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 loss of outside equipment. There may be damage from wind and flying debris. Off site, a tornado may cause a temporary loss of local utility and communications. Off-site damage is typically followed by quick restoration of services.

Tornado damage severity is measured by the Fujita Tornado Scale (Table 16.2).

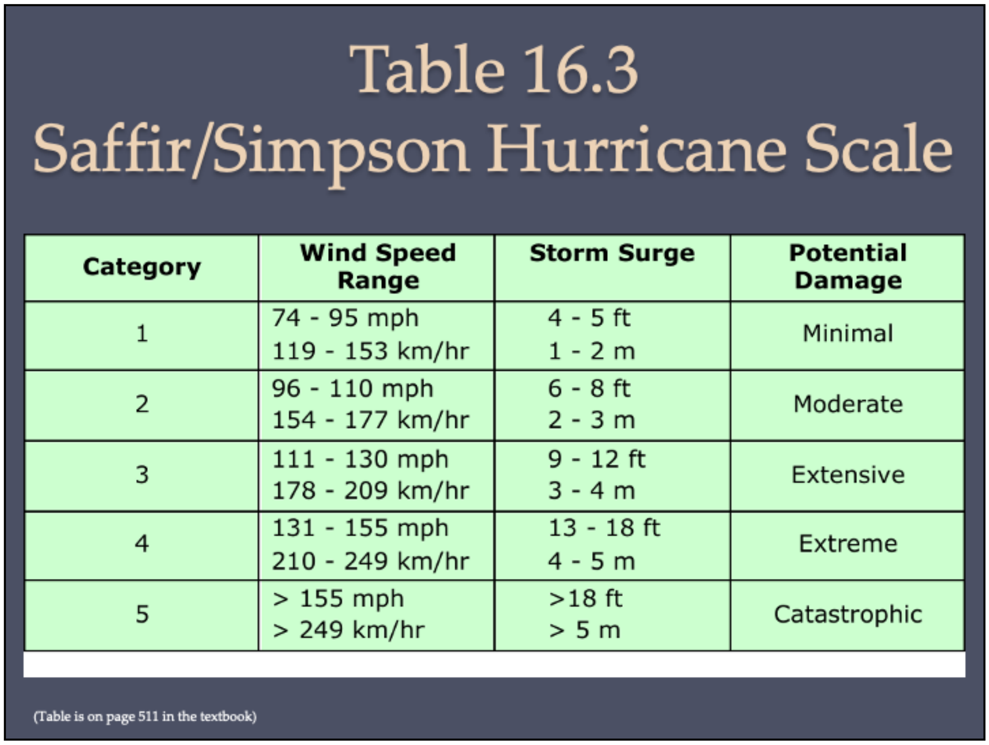


Table 16.3 Saffir/Simpson Hurricane Scale

Category	Wind Speed Range	Storm Surge	Potential Damage
1	74 - 95 mph 119 - 153 km/hr	4 - 5 ft 1 - 2 m	Minimal
2	96 - 110 mph 154 - 177 km/hr	6 - 8 ft 2 - 3 m	Moderate
3	111 - 130 mph 178 - 209 km/hr	9 - 12 ft 3 - 4 m	Extensive
4	131 - 155 mph 210 - 249 km/hr	13 - 18 ft 4 - 5 m	Extreme
5	> 155 mph > 249 km/hr	>18 ft > 5 m	Catastrophic

(Table is on page 511 in the textbook)

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. Off site, there is the potential for severe region-wide damage to public infrastructure, utilities, and communications. If on-site operation must continue, then emergency supplies for personnel as well as a backup generator are needed. Further, the responsible site manager may need to mobilize private poststorm security measures, such as armed guards.

Table 16.3 summarizes the widely used Saffir/Simpson Hurricane Scale. In general, damage rises by about a factor of four for every category increase [PIEL08].

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. Examples of inside damage include the toppling of unbraced computer hardware and site infrastructure equipment, including the collapse of raised floors. Personnel are at risk from broken glass and other flying debris. Off site, near the epicenter of a major earthquake, the damage equals and often exceeds that of a major hurricane. Structures that can withstand a hurricane, such as roads and bridges, may be damaged or destroyed, preventing the movement of fuel and other supplies.

An **ice storm** or **blizzard** can cause some disruption of or damage to IS facilities if outside equipment and the building are not designed to survive severe ice and snow accumulation. Off site, there may be widespread disruption of utilities and communications and roads may be dangerous or impassable.

The consequences of **lightning** strikes can range from no impact to disaster. The effects depend on the proximity of the strike and the efficacy of grounding and surge protection measures in place. Off site, there can be disruption of electrical power and there is the potential for fires.

Flood is a concern in areas that are subject to flooding and for facilities that are in severe flood areas at low elevation. Damage can be severe, with long-lasting effects and the need for a major cleanup operation.

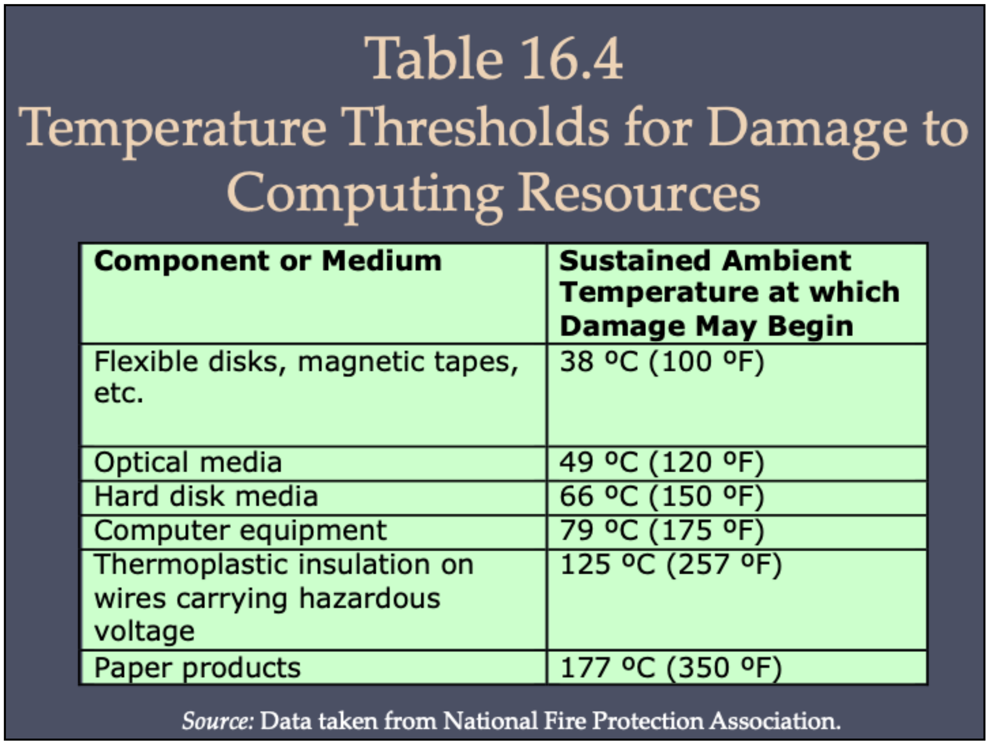


Table 16.4
Temperature Thresholds for Damage to Computing Resources

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)

Source: Data taken from National Fire Protection Association.

Computers and related equipment
are designed to operate within a certain temperature range. Most computer systems should be kept between 10 and 32 degrees Celsius (50 and 90 degrees Fahrenheit). Outside this range, resources might continue to operate but produce undesirable results. If the ambient temperature around a computer gets too high, the computer cannot adequately cool itself, and internal components can be damaged. If the temperature gets too cold, the system can undergo thermal shock when it is turned on, causing circuit boards or integrated circuits to crack. Table 16.4 indicates the point at which permanent damage from excessive heat begins.

Another concern is the internal temperature of equipment, which can be significantly higher than room temperature. Computer-related equipment comes with its own temperature dissipation and cooling mechanisms, but these may rely on, or be affected by, external conditions. Such conditions include excessive ambient temperature, interruption of supply of power or heating, ventilation, and air-conditioning (HVAC) services, and vent blockage.

High humidity also poses a threat to electrical and electronic equipment. Long-term exposure to high humidity can result in corrosion. Condensation can threaten magnetic and optical storage media. Condensation can also cause a short circuit, which in turn can damage circuit boards. High humidity can also cause a galvanic effect that results in electroplating, in which metal from one connector slowly migrates to the mating connector, bonding the two together.

Very low humidity can also be a concern. Under prolonged conditions of low humidity, some materials may change shape, and performance may be affected. Static electricity also becomes a concern. A person or object that becomes statically charged can damage electronic equipment by an electric discharge. Static electricity discharges as low as 10 volts can damage particularly sensitive electronic circuits, and discharges in the hundreds of volts can create significant damage to a variety of electronic circuits. Discharges from humans can reach into the thousands of volts, so this is a nontrivial threat.

In general, relative humidity should be maintained between 40% and 60% to avoid the threats from both low and high humidity.

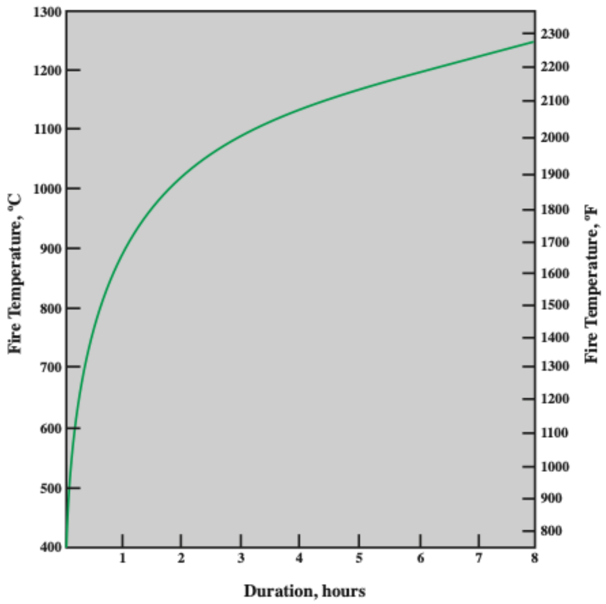


Figure 16.1 Standard Fire Temperature-Time Relations Used for Testing of Building Elements

Perhaps the most frightening physical threat is fire. It is a threat to human life and property. The threat is not only from direct flame, but also from heat, release of toxic fumes, water damage from fire suppression, and smoke damage. Further, fire can disrupt utilities, especially electricity.

The temperature due to fire increases with time, and in a typical building, fire effects follow the curve shown in Figure 16.1.

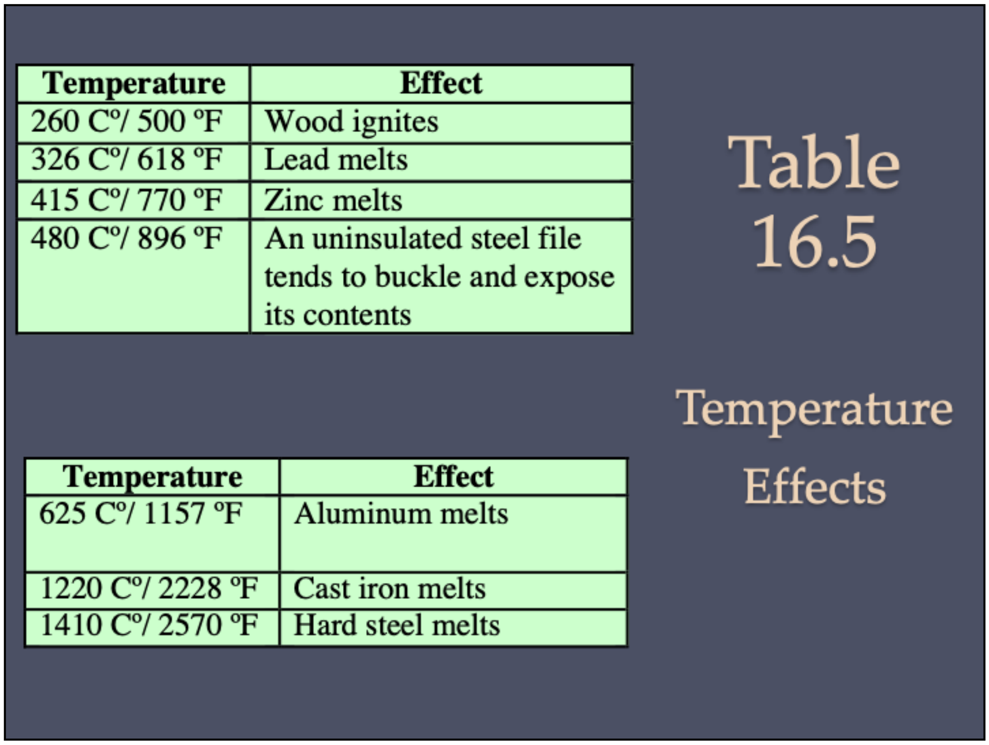


Table 16.5

Temperature Effects

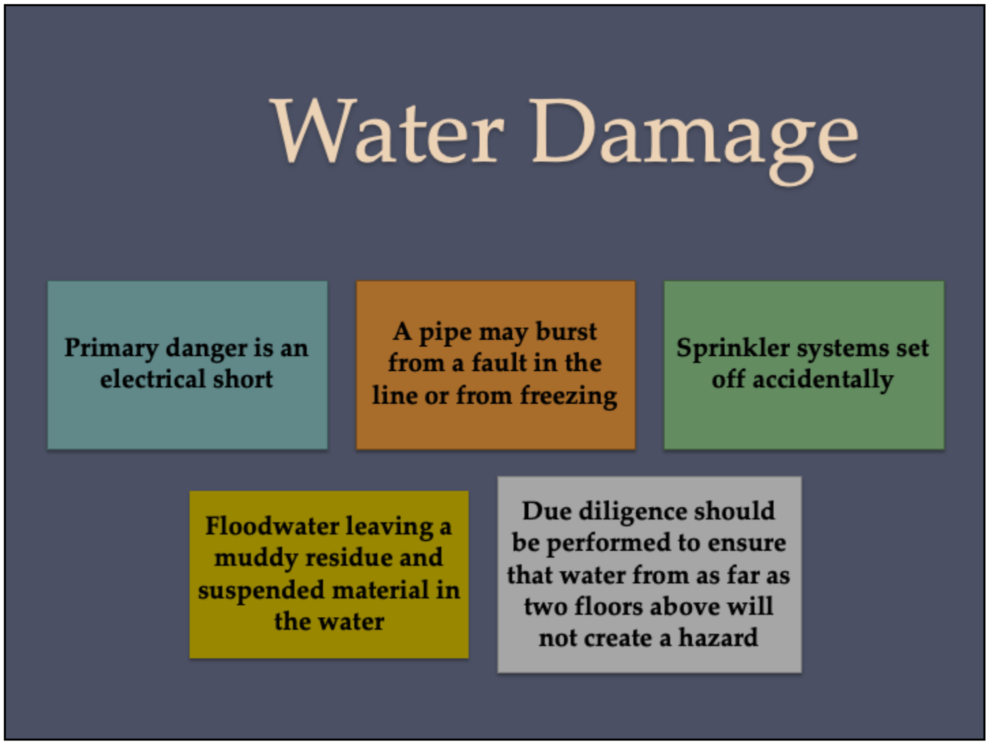
Temperature	Effect
260 C°/ 500 °F	Wood ignites
326 C°/ 618 °F	Lead melts
415 C°/ 770 °F	Zinc melts
480 C°/ 896 °F	An uninsulated steel file tends to buckle and expose its contents

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

Smoke damage related to fires can also be extensive. Smoke is an abrasive. It collects on the heads of unsealed magnetic disks, optical disks, and tape drives. Electrical fires can produce an acrid smoke that may damage other equipment and may be poisonous or carcinogenic.

The most common fire threat is from fires that originate within a facility, and, as discussed subsequently, there are a number of preventive and mitigating measures that can be taken. A more uncontrollable threat is faced from wildfires, which are a plausible concern in the western United States, portions of Australia (where the term *bushfire* is used*),* and a number of other countries.

To get a sense of the damage caused by fire, Tables 16.4 and 16.5 shows the temperature at which various items melt or are damaged and therefore indicates how long after the fire is started such damage occurs.



Water Damage

Primary danger is an electrical short

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

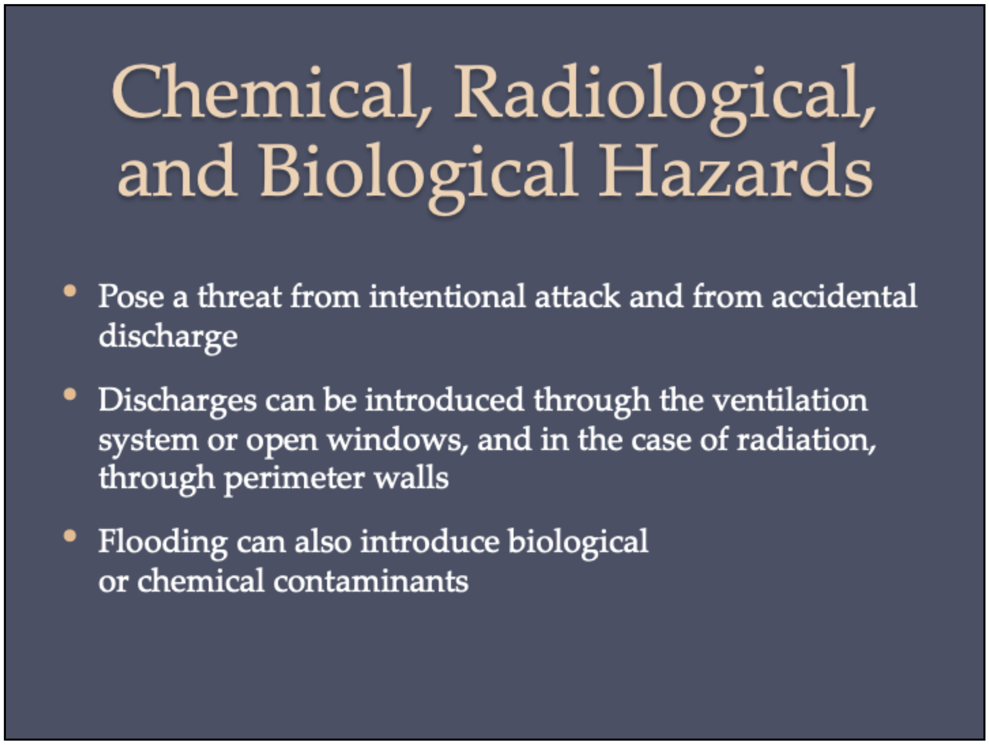
Sprinkler systems set off accidentally

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

Water and other stored liquids in proximity to computer equipment pose an obvious threat. The primary danger is an electrical short, which can happen if water bridges between a circuit board trace carrying voltage and a trace carrying ground. Moving water, such as in plumbing, and weather created water from rain, snow, and ice also pose threats. A pipe may burst from a fault in the line or from freezing. Sprinkler systems, despite their security function, are a major threat to computer equipment and paper and electronic storage media. The system may be set off by a faulty temperature sensor, or a burst pipe may cause water to enter the computer room. In any large computer installation, due diligence should be performed to ensure that water from as far as two floors above will not create a hazard. An overflowing toilet is an example of such a hazard.

Less common, but more catastrophic, is floodwater. Much of the damage comes from the suspended material in the water. Floodwater leaves a muddy residue that is extraordinarily difficult to clean up.

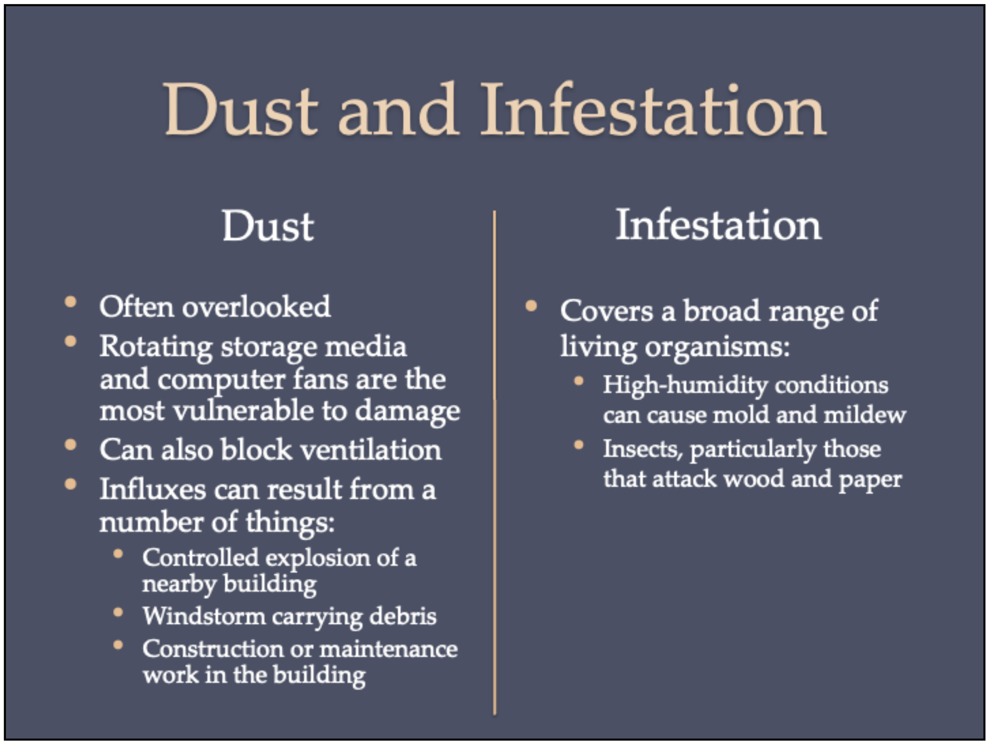


Chemical, Radiological, and Biological Hazards

- Pose a threat from intentional attack and from accidental discharge
- Discharges can be introduced through the ventilation system or open windows, and in the case of radiation, through perimeter walls
- Flooding can also introduce biological or chemical contaminants

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

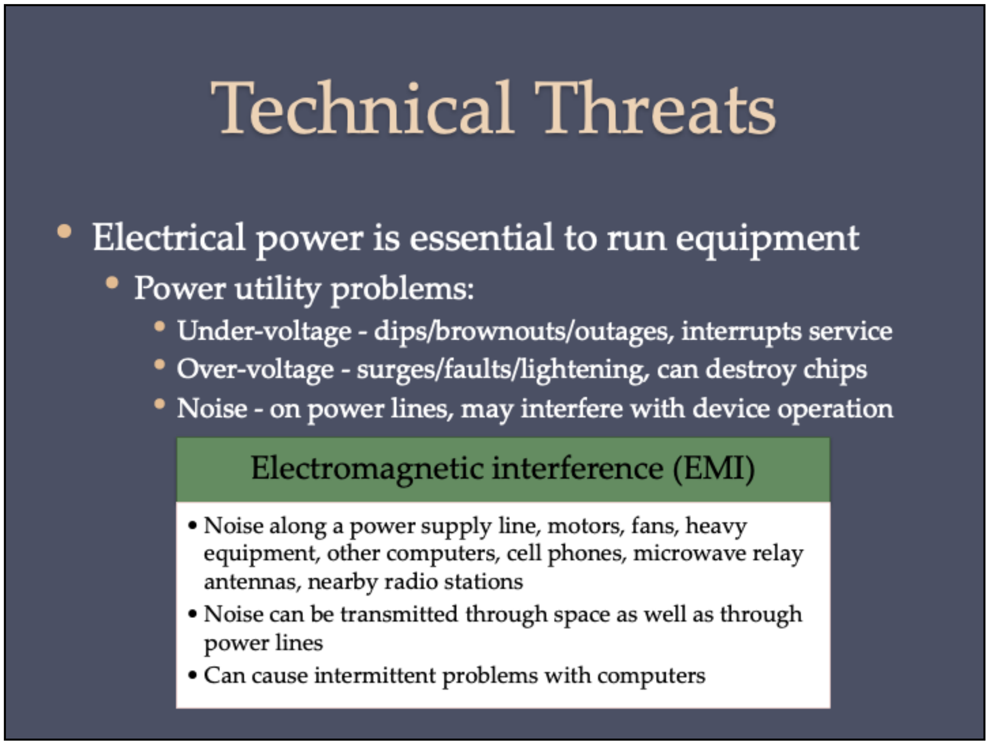
Infestation

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

Dust is a prevalent concern that is often overlooked. Even fibers from fabric and paper are abrasive and mildly conductive, although generally equipment is resistant to such contaminants. Larger influxes of dust can result from a number of incidents, such as a controlled explosion of a nearby building and a windstorm carrying debris from a wildfire. A more likely source of influx comes from dust surges that originate within the building due to construction or maintenance work.

Equipment with moving parts, such as rotating storage media and computer fans, are the most vulnerable to damage from dust. Dust can also block ventilation and reduce radiational cooling.

One of the less pleasant physical threats is infestation, which covers a broad range of living organisms, including mold, insects, and rodents. High-humidity conditions can lead to the growth of mold and mildew, which can be harmful to both personnel and equipment. Insects, particularly those that attack wood and paper, are also a common threat.



Technical Threats

- Electrical power is essential to run equipment
  - Power utility problems:
    - Under-voltage - dips/brownouts/outages, interrupts service
    - Over-voltage - surges/faults/lightening, can destroy chips
    - Noise - on power lines, may interfere with device operation

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

This category encompasses threats related to electrical power and electromagnetic emission.

Electrical power is essential to the operation of an information system. All of the electrical and electronic devices in the system require power, and most require uninterrupted utility power. Power utility problems can be broadly grouped into three categories: undervoltage, overvoltage, and noise.

An **undervoltage** 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. Deeper dips or blackouts lasting more than a few milliseconds trigger a system shutdown. Generally, no damage is done, but service is interrupted.

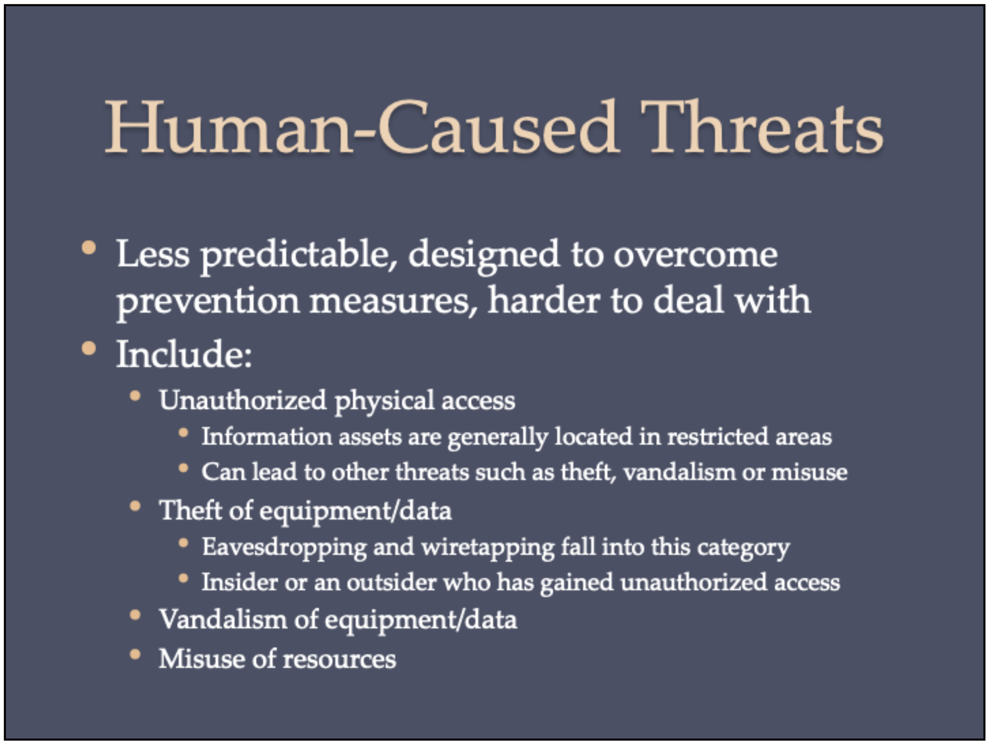
Far more serious is an **overvoltage** condition. A surge of voltage can be caused

by a utility company supply anomaly, by some internal (to the building) wiring fault, or
by lightning. Damage is a function of intensity and duration, and the effectiveness of any surge protectors between your equipment and the source of the surge. A sufficient surge can destroy silicon-based components, including processors and memories.

Power lines can also be a conduit for **noise.** In many cases, these spurious signals can endure through the filtering circuitry of the power supply and interfere with signals inside electronic devices, causing logical errors.

Noise along a power supply line is only one
source of electromagnetic interference (EMI). Motors, fans, heavy equipment, and even other computers generate electrical noise that can cause intermittent problems with the computer you are using. This noise can be transmitted through space as well as through nearby power lines.

Another source of EMI is high-intensity emissions from nearby commercial radio stations and microwave relay antennas. Even low-intensity devices, such as cellular telephones, can interfere with sensitive electronic equipment.



Human-Caused Threats

- Less predictable, designed to overcome prevention measures, harder to deal with
- Include:
  - Unauthorized physical access
    - Information assets are generally located in restricted areas
    - Can lead to other threats such as theft, vandalism or misuse
  - Theft of equipment/data
    - Eavesdropping and wiretapping fall into this category
    - Insider or an outsider who has gained unauthorized access
  - Vandalism of equipment/data
  - Misuse of resources

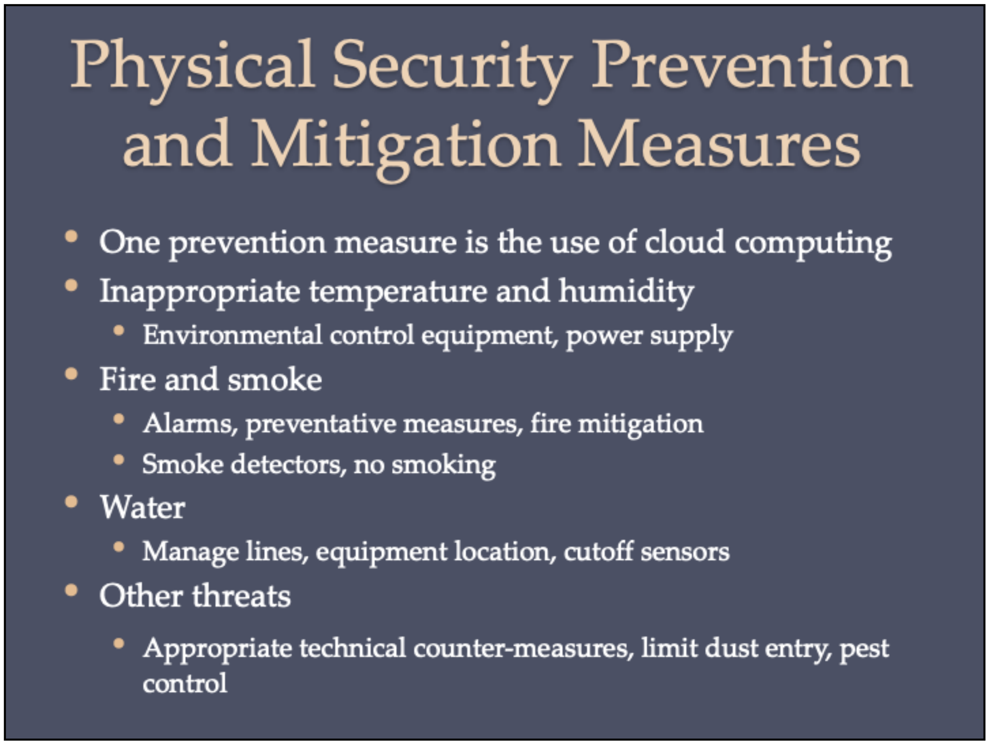
Human-caused threats are more difficult to deal with than the environmental and technical threats discussed so far. Human-caused threats are less predictable than other types of physical threats. Worse, human-caused threats are specifically designed to overcome prevention measures and/or seek the most vulnerable point of attack. We can group such threats into the following categories:

• **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 to use the resources at all.



Physical Security Prevention and Mitigation Measures

- One prevention measure is the use of cloud computing
- Inappropriate temperature and humidity
  - Environmental control equipment, power supply
- Fire and smoke
  - Alarms, preventative measures, fire mitigation
  - Smoke detectors, no smoking
- Water
  - Manage lines, equipment location, cutoff sensors
- Other threats
  - Appropriate technical counter-measures, limit dust entry, pest control

In this section, we look at a range of techniques for preventing, or in some cases simply deterring, physical attacks. We begin with a survey of some of the techniques for dealing with environmental and technical threats and then move on to human-caused threats. Standards including ISO 27002 (*Code of practice for information security management*, 2013) and NIST SP 800-53 (*Recommended Security Controls for Federal Information Systems*, January 2015) include lists of controls relating to physical and environmental security, as we showed in Tables 15.2 and 15.3.

One general prevention measure is the use of cloud computing. From a physical security viewpoint, an obvious benefit of cloud computing is that there is a reduced need for information system assets on site and a substantial portion of data assets are not subject to on-site physical threats. See Chapter 13 for a discussion of cloud computing security issues.

Dealing with this problem is primarily a matter of having environmental-control

equipment of appropriate
capacity and appropriate sensors to warn of thresholds being exceeded. Beyond that, the principal requirement is the maintenance of a power supply, discussed subsequently.

Dealing with fire involves a combination of alarms, preventive
measures, and fire mitigation. [MART73] provides the following list of necessary measures:

1. Choice of site to minimize likelihood of disaster. Few disastrous fires originate in a well-protected computer room or IS facility. The IS area should be chosen to minimize fire, water, and smoke hazards from adjoining areas. Common walls with other activities should have at least a one-hour fire-protection rating.

2. Air conditioning and other ducts designed so as not to spread fire. There are standard guidelines and specifications for such designs.

3. Positioning of equipment to minimize damage.

4. Good housekeeping. Records and flammables must not be stored in the IS area. Tidy installation if IS equipment is crucial.

5. Hand-operated fire extinguishers readily available, clearly marked, and regularly tested.

6. Automatic fire extinguishers installed. Installation should be such that the extinguishers are unlikely to cause damage to equipment or danger to personnel.

7. Fire detectors. The detectors sound alarms inside the IS room and with external authorities, and start automatic fire extinguishers after a delay to

permit human intervention.

8. Equipment power-off switch. This switch must be clearly marked and unobstructed. All personnel must be familiar with power-off procedures.

9. Emergency procedures posted.

10. Personnel safety. Safety must be considered in designing the building layout and emergency procedures.

11. Important records stored in fireproof cabinets or vaults.

12. Records needed for file reconstruction stored off the premises.

13. Up-to-date duplicate of all programs stored off the premises.

14. Contingency plan for use of equipment elsewhere should the computers be destroyed.

15. Insurance company and local fire department should inspect the facility.

To deal with the threat of smoke, the responsible manager should install smoke detectors in every room that contains computer equipment as well as under raised floors and over suspended ceilings. Smoking should not be permitted in computer rooms.

For wildfires, the available countermeasures are limited. Fire-resistant building techniques are costly and difficult to justify.

Prevention and mitigation measures for water threats must encompass the range of such threats. For plumbing leaks, the cost of relocating threatening lines is generally difficult to justify. With knowledge of the exact layout of water supply lines, measures can be taken to locate equipment sensibly. The location of all shutoff valves should be clearly visible or at least clearly documented, and responsible personnel should know the procedures to follow in case of emergency.

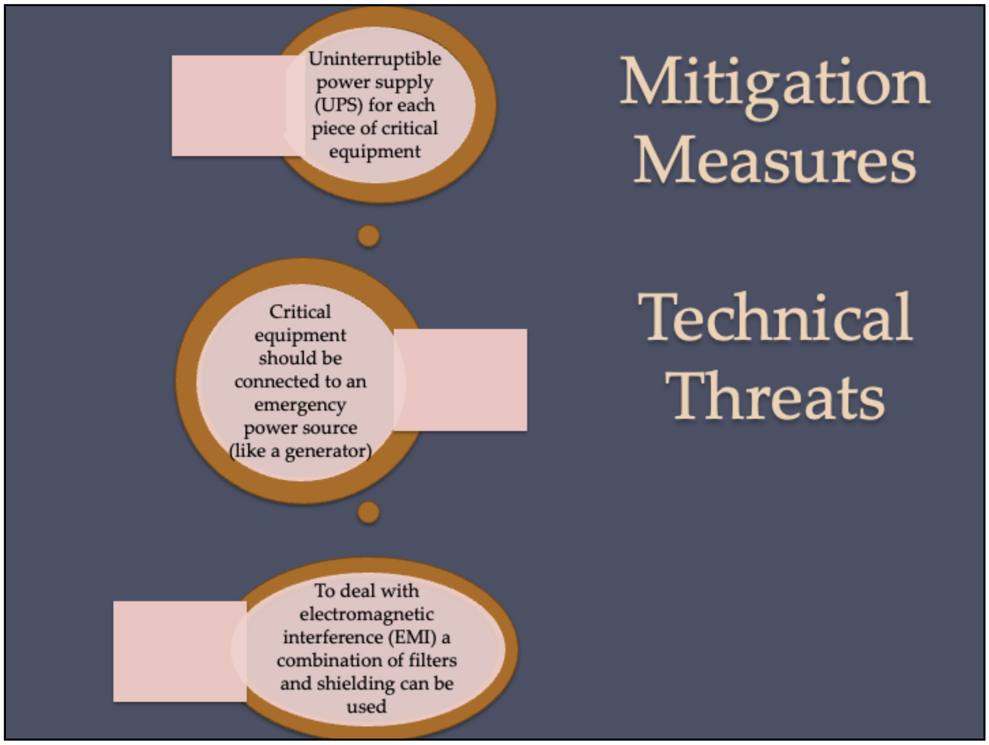
To deal with both plumbing leaks and other sources of water, sensors are vital. Water sensors should be located on the floor of computer rooms, as well as under raised floors, and should cut off power automatically in the event of a flood.

For chemical, biological, and radiological threats, specific technical approaches are available, including infrastructure design, sensor design and placement, mitigation procedures, personnel training, and so

forth. Standards and techniques in these areas continue to evolve.

As for dust hazards, the obvious prevention method is to limit dust through proper filter maintenance and regular IS room maintenance.

For infestations, regular pest control procedures may be needed, starting with maintaining a clean environment.



Mitigation Measures

Technical Threats

Uninterruptible power supply (UPS) for each piece of critical equipment

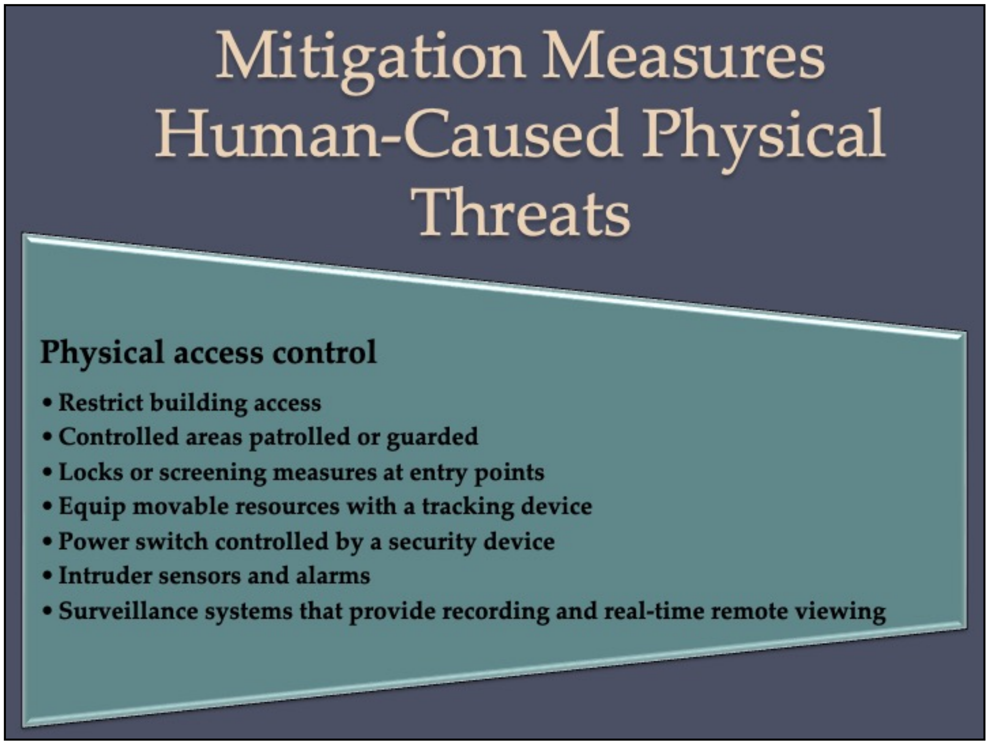
Critical equipment should be connected to an emergency power source (like a generator)

To deal with electromagnetic interference (EMI) a combination of filters and shielding can be used

To deal with brief power interruptions, an uninterruptible power supply (UPS) should be employed for each piece of critical equipment. The UPS is a battery backup unit that can maintain power to processors, monitors, and other equipment for a period of minutes. UPS units can also function as surge protectors, power noise filters, and automatic shutdown devices when the battery runs low.

For longer blackouts or brownouts, critical equipment should be connected to an emergency power source, such as a generator. For reliable service, a range of issues need to be addressed by management, including product selection, generator placement, personnel training, testing and maintenance schedules, and so forth.

To deal with electromagnetic interference, a combination of filters and shielding can be used. The specific technical details will depend on the infrastructure design and the anticipated sources and nature of the interference.



Mitigation Measures Human-Caused Physical Threats

Physical access control

- Restrict building access
- Controlled areas patrolled or guarded
- Locks or screening measures at entry points
- Equip movable resources with a tracking device
- Power switch controlled by a security device
- Intruder sensors and alarms
- Surveillance systems that provide recording and real-time remote viewing

The general approach to human-caused physical threats is physical access control. Based on [MICH06], we can suggest a spectrum of approaches that can be used to restrict access to equipment. These methods can be used in combination.

1. Physical contact with a resource is restricted by restricting access to the building in which the resource is housed. This approach is intended to deny access to outsiders but does not address the issue of unauthorized insiders or employees.

2. Physical contact with a resource is restricted by putting the resource in a locked cabinet, safe, or room.

3. A machine may be accessed, but it is secured (perhaps permanently bolted) to an object that is difficult to move. This will deter theft but not vandalism, unauthorized access, or misuse.

4. A security device controls the power switch.

5. A movable resource is equipped with a tracking device so that a sensing portal can alert security personnel or trigger an automated barrier to prevent the object from being moved out of its proper security area.

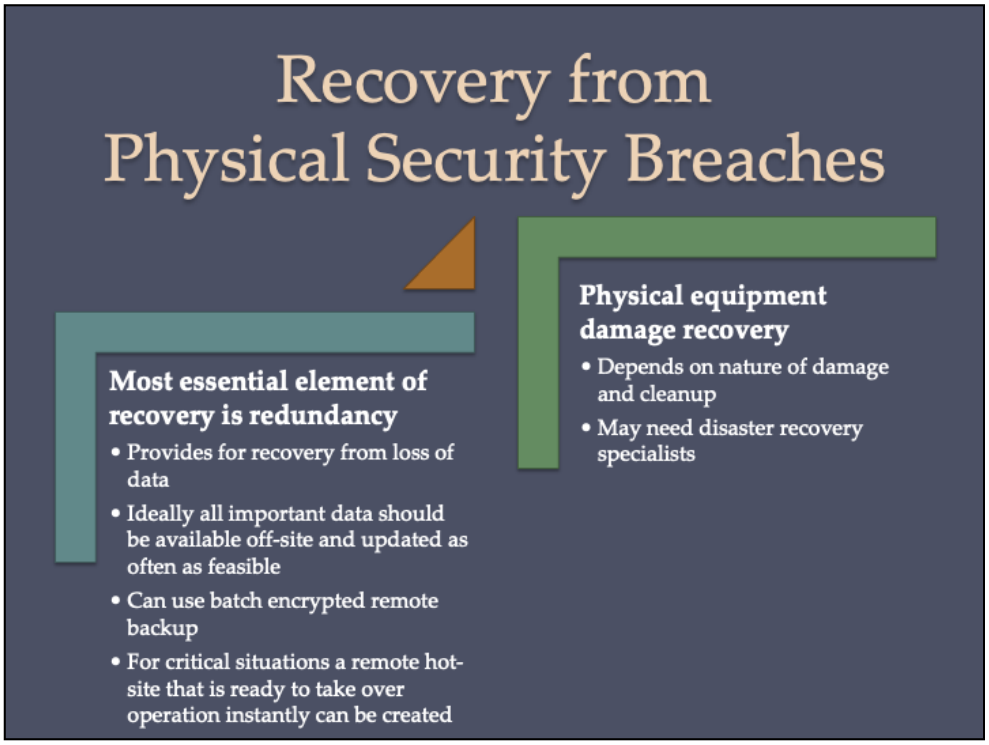
6. A portable object is equipped with a tracking device so that its current position can be monitored continually.

The first two of the preceding approaches isolate the equipment. Techniques that can be used for this type of access control include controlled areas patrolled or guarded by personnel, barriers that isolate each area, entry points in the barrier (doors), and locks or screening measures at each entry point.

Physical access control should address not just computers and other IS equipment but also locations of wiring used to connect systems, the electrical power service, the HVAC equipment and distribution system, telephone and communications lines, backup media, and documents.

In addition to physical and procedural barriers, an effective physical access control regime includes a variety of sensors and alarms to detect intruders and unauthorized access or movement of equipment. Surveillance systems are frequently an integral part of building security, and special-purpose surveillance systems for the IS area are generally also warranted. Such systems should provide real-time remote viewing as well as recording.

Finally, the introduction of Wi-Fi changes the concept of physical security in the sense that it extends physical access across physical boundaries such as walls and locked doors. For example, a parking lot outside of a secure building provides access via Wi-Fi. This type of threat and the measures to deal with it are discussed in Chapter 24.



Recovery from Physical Security Breaches

Most essential element of recovery is redundancy

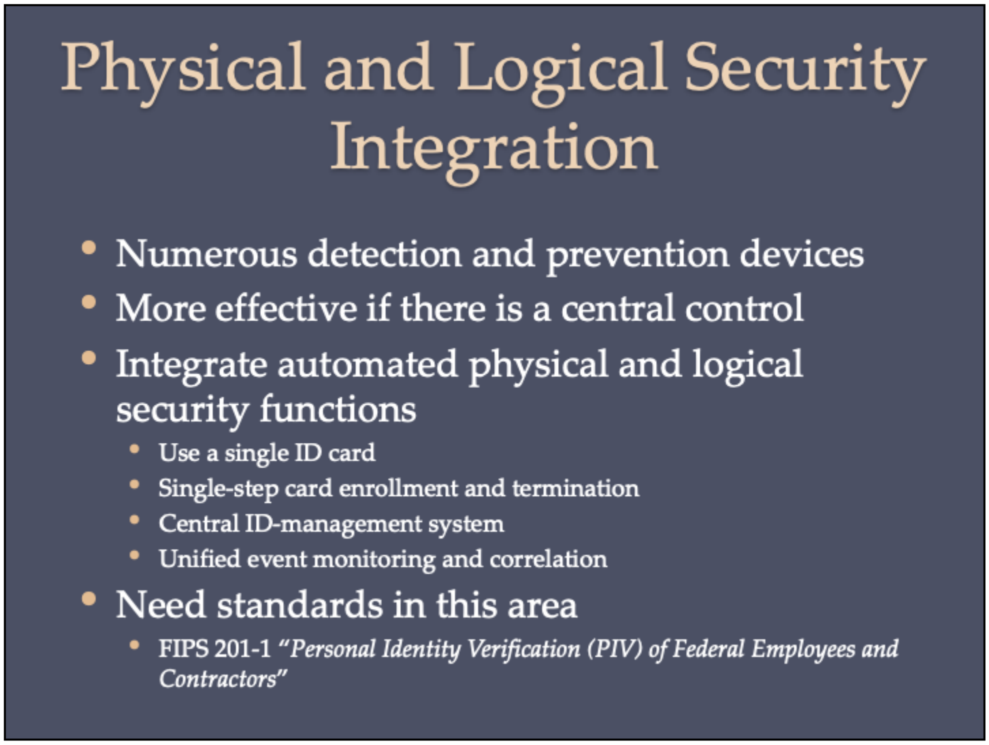
- Provides for recovery from loss of data
- Ideally all important data should be available off-site and updated as often as feasible
- Can use batch encrypted remote backup
- For critical situations a remote hot-site that is ready to take over operation instantly can be created

Physical equipment damage recovery

- Depends on nature of damage and cleanup
- May need disaster recovery specialists

The most essential element of recovery from physical security breaches is redundancy. Redundancy does not undo any breaches of confidentiality, such as the theft of data or documents, but it does provide for recovery from loss of data. Ideally, all of the important data in the system should be available off site and updated as near to real time as is warranted based on a cost/benefit trade-off. With broadband connections now almost universally available, batch encrypted backups over private networks or the Internet are warranted and can be carried out on whatever schedule is deemed appropriate by management. In the most critical situations, a *hot site can* be created off site that is ready to take over operation instantly and has available to it a near-real-time copy of operational data.

Recovery from physical damage to the equipment or the site depends on the nature of the damage and, importantly, the nature of the residue. Water, smoke, and fire damage may leave behind hazardous materials that must be meticulously removed from the site before normal operations and the normal equipment suite can be reconstituted. In many cases, this requires bringing in disaster recovery specialists from outside the organization to do the cleanup.



Physical and Logical Security Integration

- Numerous detection and prevention devices
- More effective if there is a central control
- Integrate automated physical and logical security functions
  - Use a single ID card
  - Single-step card enrollment and termination
  - Central ID-management system
  - Unified event monitoring and correlation
- Need standards in this area
  - FIPS 201-1 *"Personal Identity Verification (PIV) of Federal Employees and Contractors"*

Physical security involves numerous detection devices, such as sensors and alarms, and numerous prevention devices and measures, such as locks and physical barriers. It should be clear that there is much scope for automation and for the integration of various computerized and electronic devices. Clearly, physical security can be made more effective if there is a central destination for all alerts and alarms and if there is central control of all automated access control mechanisms, such as smart card entry sites.

From the point of view of both effectiveness and cost, there is increasing interest not only in integrating automated physical security functions but in integrating, to the extent possible, automated physical and logical security functions. The most promising area is that of access control. Examples of ways to integrate physical and logical access control include the following:

• Use of a single ID card for physical and logical access. This can be a simple magnetic-strip card or a smart card.

• Single-step user/card enrollment and termination across all identity and access control databases.

• A central ID-management system instead of multiple disparate user directories and databases.

• Unified event monitoring and correlation.

As an example of the utility of this integration, suppose that an alert indicates that Bob has logged on to the company's wireless network (an event generated by the logical access control system) but did not enter the building (an event generated from the physical access control system). Combined, these two events suggest that someone is hijacking Bob's wireless account.

For the integration of physical and logical access control to be practical, a wide range of vendors must conform to standards that cover smart card protocols, authentication and access control formats and protocols, database entries, message formats, and so on. An important step in this direction is FIPS 201-2 [*Personal Identity Verification* (*PIV) of Federal Employees and Contractors], issued by NIST in 2013.* This standard defines a reliable, government-wide PIV system for use in applications such as access to federally controlled facilities and information systems. The standard specifies a PIV system within which common identification credentials can be created and later used to verify a claimed identity. The standard also identifies Federal government-wide requirements for security levels that are dependent on risks to the facility or information being protected. The standard applies to private-sector contractors as well, and serves as a useful guideline for any organization.

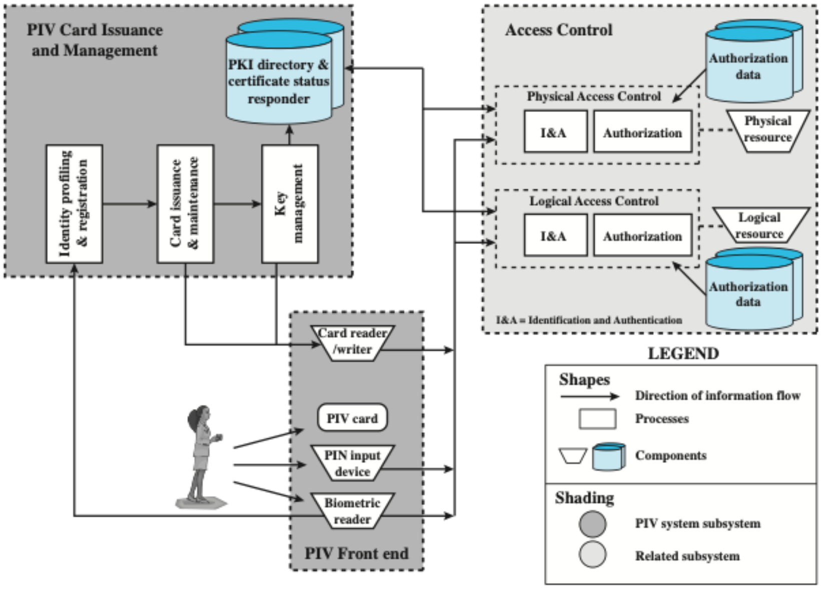


Figure 16.2 FIPS 201 PIV System Model

Figure 16.2 illustrates the major components of FIPS 201-2 compliant systems. The PIV front end defines the physical interface to a user who is requesting access to a facility, which could be either physical access to a protected physical area or logical access to an information system. The **PIV front end subsystem** supports up to three factor

authentication; the number of factors used depends on the level of security required. The front end makes use of a smart card, known as a PIV card, which is a dual-interface contact and contactless card. The card holds a cardholder photograph, X.509 certificates, cryptographic keys, biometric data, and a cardholder unique identifier

(CHUID), explained subsequently. Certain cardholder information may be read-protected and require a personal identification number (PIN) for read access by the card reader. The biometric reader, in the current version of the standard, is a fingerprint reader or an iris scanner.

The standard defines three assurance levels for verification of the card and the encoded data stored on the card, which in turn leads to verifying the authenticity of the person holding the credential. A level of *some confidence* corresponds to use of the card reader and PIN. A level of *high confidence* adds a biometric comparison of a fingerprint captured and encoded on the card during the card-issuing process and a fingerprint scanned at the physical access point. A *very high confidence* level requires that the process just described is completed at a control point attended by an official observer.

The other major component of the PIV system is the **PIV card issuance and management subsystem .** This subsystem includes the components responsible for identity proofing and registration, card and key issuance and management, and the various repositories and services (e.g., public key infrastructure [PKI] directory, certificate status servers) required as part of the verification infrastructure.

The PIV system interacts with an **access control subsystem,** which includes components responsible for determining a particular PIV cardholder's access to a physical or logical resource. FIPS 201-2 standardizes data formats and protocols for interaction between the PIV system and the access control system.

Unlike the typical card number/facility code encoded on most access control cards, the FIPS 201-2 CHUID takes authentication to a new level, through the use of an expiration date (a required CHUID data field) and an optional CHUID digital signature. A digital signature can be checked to ensure that the CHUID recorded on the card was digitally signed by a trusted source and that the CHUID data have not been altered since the card was signed. The CHUID expiration date can be checked to verify that the card has not expired. This is independent from whatever expiration date is associated with cardholder privileges. Reading and verifying the CHUID alone provides only some assurance of identity because it authenticates the card data, not the cardholder. The PIN and biometric factors provide identity verification of the individual.

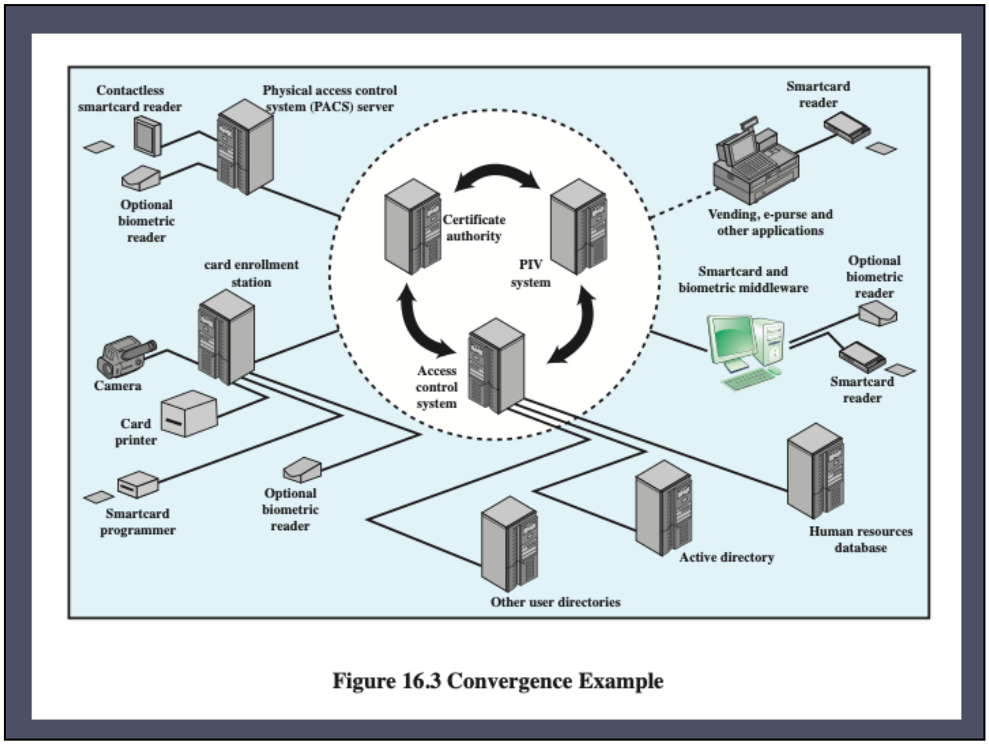

Contactless smartcard reader
Physical access control system (PACS) server
Smartcard reader
Optional biometric reader
Certificate authority
PIV system
Vending, e-purse and other applications
card enrollment station
Smartcard and biometric middleware
Optional biometric reader
Camera
Access control system
Smartcard reader
Card printer
Smartcard programmer
Optional biometric reader
Human resources database
Active directory
Other user directories

Figure 16.3 Convergence Example

Figure 16.3 , based on [FORR06], illustrates the convergence of physical and logical access control using FIPS 201-2. The core of the system includes the PIV and access control system as well as a certificate authority for signing CHUIDs. The other elements of the figure provide examples of the use of the system core for integrating physical and logical access control.

If the integration of physical and logical access control extends beyond a unified front end to an integration of system elements, a number of benefits accrue, including the following [FORR06]:

• Employees gain a single, unified access control authentication device; this cuts down on misplaced tokens, reduces training and overhead, and allows seamless access.

• A single logical location for employee ID management reduces duplicate data entry operations and allows for immediate and real-time authorization revocation of all enterprise resources.

- Auditing and forensic groups have a central repository for access control investigations.

- Hardware unification can reduce the number of vendor purchase-and-support contracts.

- Certificate-based access control systems can leverage user ID certificates for other security applications, such as document e-signing and data encryption.

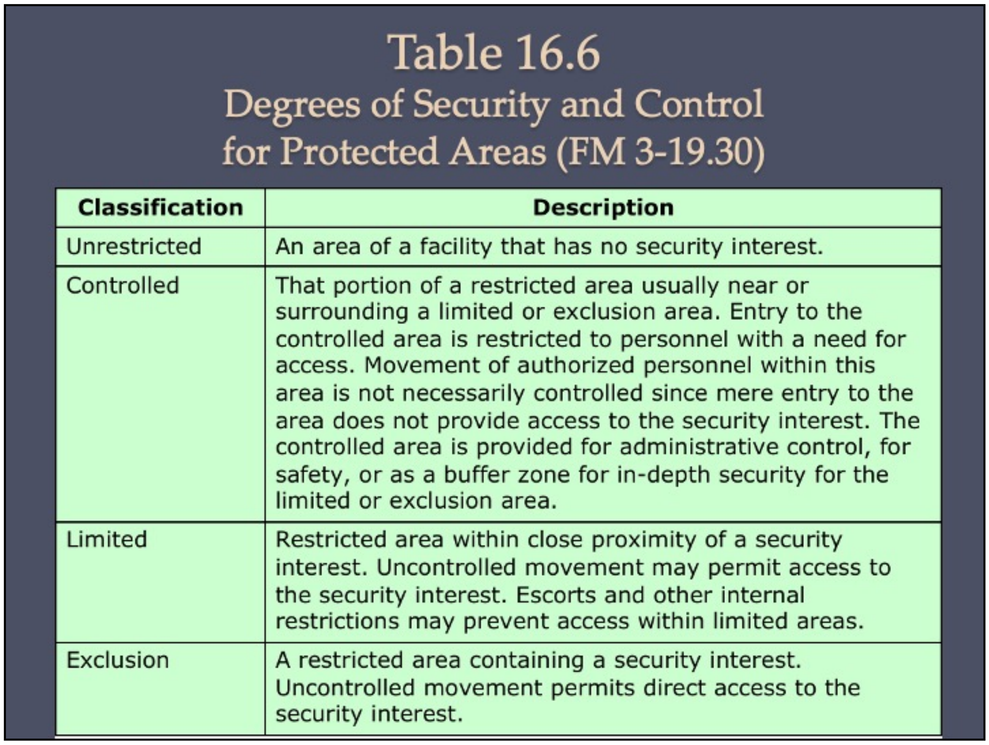


Table 16.6
Degrees of Security and Control for Protected Areas (FM 3-19.30)

Classification	Description
Unrestricted	An area of a facility that has no security interest.
Controlled	That portion of a restricted area usually near or surrounding a limited or exclusion area. Entry to the controlled area is restricted to personnel with a need for access. Movement of authorized personnel within this area is not necessarily controlled since mere entry to the area does not provide access to the security interest. The controlled area is provided for administrative control, for safety, or as a buffer zone for in-depth security for the limited or exclusion area.
Limited	Restricted area within close proximity of a security interest. Uncontrolled movement may permit access to the security interest. Escorts and other internal restrictions may prevent access within limited areas.
Exclusion	A restricted area containing a security interest. Uncontrolled movement permits direct access to the security interest.

FIPS 201-2 defines characteristics of the identity credential that can be interoperable government-wide. It does not, however, provide specific guidance for applying this standard as part of a physical access control system (PACS) in an environment in which one or more levels of access control is desired. To provide such guidance, in NIST SP 800-116 [*A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS) 2008),* was issued and is being revised as of 2017.

SP 800-116 makes use of the following authentication mechanisms:

• **Visual (VIS):** Visual identity verification of a PIV card is done by a human guard. The human guard checks to see that the PIV card looks genuine, compares the cardholder's facial features with the picture on the card, checks the expiration date printed on the card, verifies the correctness of other data elements printed on the card, and visually verifies the security feature(s) on the card.

• **Cardholder unique identifier (CHUID):** The CHUID is a PIV card data object. Authentication is implemented by transmission of the CHUID from the PIV card to PACS.

• **Biometric (BIO):** Authentication is implemented by using a fingerprint or iris data object sent from the PIV card to the PACS.

• **Attended biometric (BIO-A):** This authentication mechanism is the same as BIO authentication but an attendant supervises the use of the PIV card and the submission of the PIN and the sample biometric by the cardholder.

• **PIV authentication key (PKI):** PACS may be designed to perform public key cryptography-based authentication using the PIV authentication key. Use of the PKI provides two-factor authentication, since the cardholder must enter a PIN to unlock the card in order to successfully authenticate.

• **Card authentication key (CAK):** The CAK is an optional key that may be present on any PIV card. The purpose of the CAK authentication mechanism is to authenticate the card and therefore its possessor. The CAK is unique among the PIV keys in several respects: The CAK may be used on the contactless or contact interface in a challenge/response protocol; and the use of the CAK does not require PIN entry.

All of these authentication mechanisms, except for CAK, are defined in FIPS 201-2. CAK is an optional PIV mechanism defined in SP800-116. SP800-116 is designed to address an environment in which different physical access points within a facility do not all have the same security requirements, and therefore the PIV authentication mechanism should be selected to conform to the security requirements of the different protected areas.

SP 800-116 recommends that authentication mechanisms be selected on the basis of protective areas established around assets or resources. The document adopts the concept of "Controlled, Limited, Exclusion" areas, as defined in [ARMY10] and summarized in Table 16.6 . Procedurally, proof of affiliation is often sufficient to gain access to a controlled area (e.g., an agency's badge to that agency's headquarters' outer perimeter). Access to limited areas is often based on functional subgroups or roles (e.g., a division badge to that division's building or wing). The individual membership in the group or privilege of the role is established by authentication of the identity of the cardholder. Access to exclusion areas may be gained by individual authorization only.

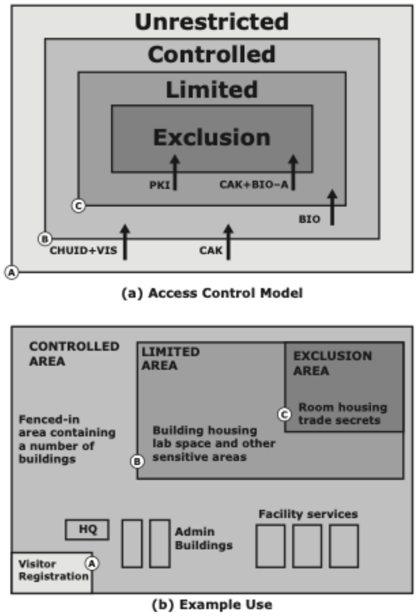
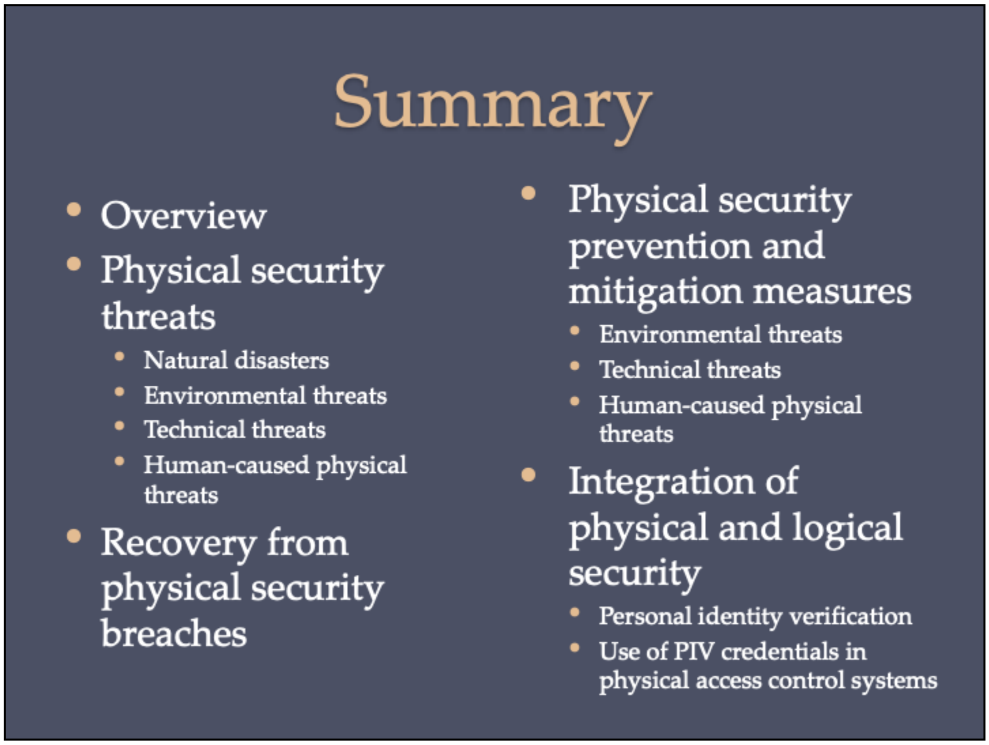


Figure 16.4 Use of Authentication Mechanisms for Physical Access Control

Figure 16.4a illustrates a general model defined in SP 800-116. The model indicates alternative authentication mechanisms that may be used for access to specific areas. The model is designed such that at least one authentication factor is required to enter a controlled area, two factors for a limited area, and three factors for an exclusion area.

Figure 16.4b is an example of the application of SP800-116 principles to a commercial, academic, or government facility. A visitor registration area is available to all. In this example, the entire facility beyond visitor registration is a controlled area available to authorized personnel and their visitors. This may be considered a relatively low-risk area, in which some confidence in the identity of those entering should be achieved. A one-factor authentication mechanism, such as CHUID+VIS or CAK, would be an appropriate security measure for this portion of the facility. Within the controlled area is a limited area restricted to a specific group of individuals. This may be considered a moderate-risk facility and a PACS should provide additional security to the more valuable assets. High confidence in the identity of the cardholder should be achieved for access. Implementation of BIO-A or PKI authentication mechanisms would be an appropriate countermeasure for the limited area. Combined with the authentication at access point A, this provides two-factor authentication to enter the limited area. Finally, within the limited area is a high-risk exclusion area restricted to a specific list of individuals. The PACS should provide very high confidence in the identity of a cardholder for access to the exclusion area. This could be provided by adding a third authentication factor, different from those used at access points A and B.

The model illustrated in Figure 16.4a , and the example in Figure 16.4b , depicts a nested arrangement of restricted areas. This arrangement may not be suitable for all facilities. In some facilities, direct access from outside to a limited area or an exclusion area may be necessary. In that case, all of the required authentication factors must be employed at the access point. Thus a direct access point to an exclusion area may employ, in combination, CHUID+VIS, BIO or BIO-A, and PKI.



Summary

- Overview
- Physical security threats
  - Natural disasters
  - Environmental threats
  - Technical threats
  - Human-caused physical threats
- Recovery from physical security breaches
- Physical security prevention and mitigation measures
  - Environmental threats
  - Technical threats
  - Human-caused physical threats
- Integration of physical and logical security
  - Personal identity verification
  - Use of PIV credentials in physical access control systems

Chapter 16 summary.