

# Week 12

---

PHYSICAL AND INFRASTRUCTURE SECURITY  
HUMAN RESOURCES SECURITY

# Chapter 16

## Physical and Infrastructure Security

# Physical and Infrastructure Security

---

## Logical security

- Protects computer-based data from software-based and communication-based threats

## Physical security

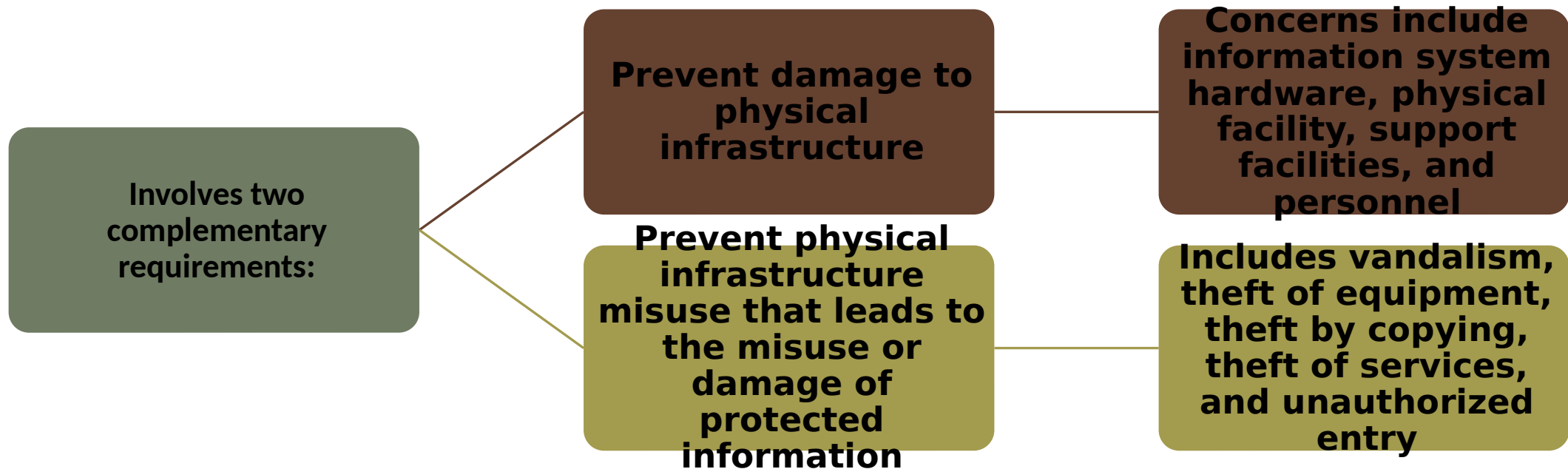
- Also called infrastructure security
- Protects the information systems that contain data and the people who use, operate, and maintain the systems
- Must prevent any type of physical access or intrusion that can compromise logical security

## 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 Overview

---



Protect physical assets that support the storage and processing of information

# Physical Security Threats

---

Physical situations and occurrences that threaten information systems:

- Environmental threats
- Technical threats
- Human-caused threats

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

# Characteristics of Natural Disasters

---

| Category | Wind Speed Range                 | Description of Damage  |
|----------|----------------------------------|--|
| F0       | 40 - 72 mph<br>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<br>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<br>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<br>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<br>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<br>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. |

# Fujita Tornado Intensity Scale

---

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

# Saffir/ Simpson Hurricane Scale

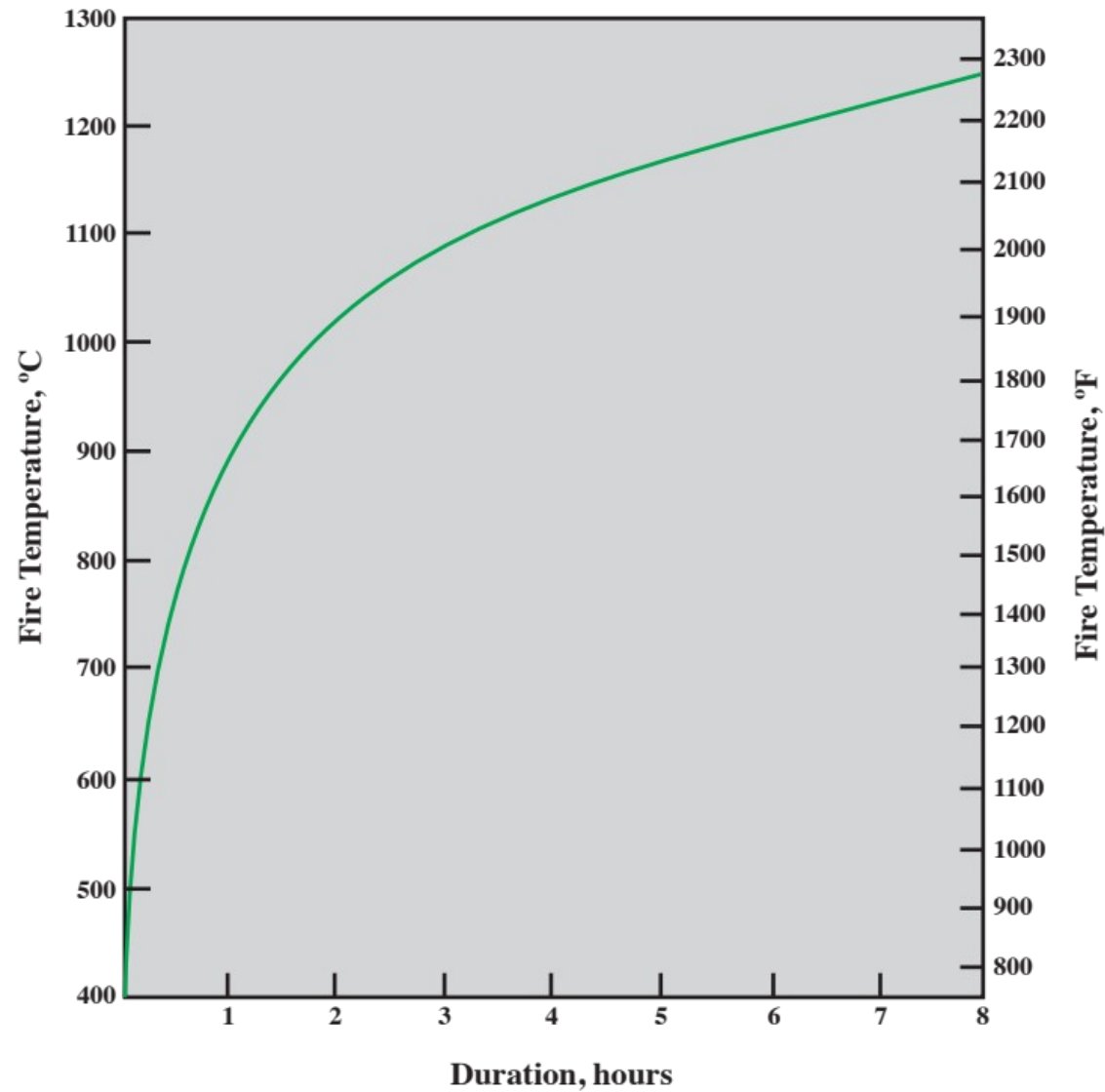
---



| <b>Component or Medium</b>                                   | <b>Sustained Ambient Temperature at which Damage May Begin</b> |
|--|--|
| 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 Thresholds for Damage to Computing Resources

---



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

# Standard Fire-Temperature Time Relations

---

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

| 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 Effects

---

# 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**

# 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

# 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 Issues

---

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

# 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



# 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

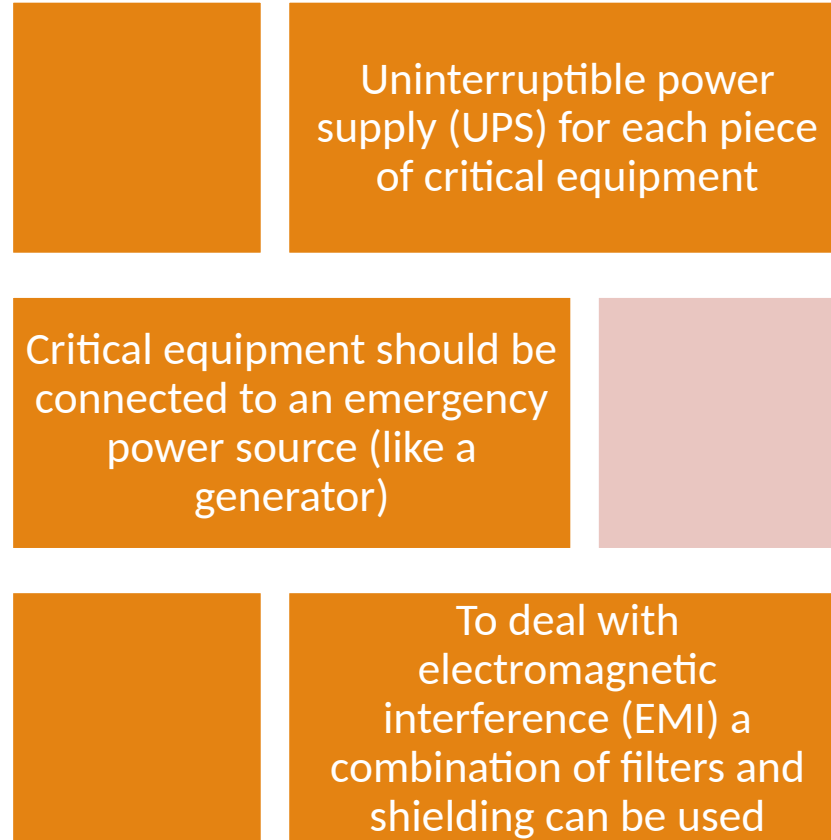
- Manage lines, equipment location, cutoff sensors

Other threats

- Appropriate technical counter-measures, limit dust entry, pest control

# Mitigation Measures – Technical Threats

---



# Mitigation Measures – Human 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

### 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

# Recovery from Physical Security Breaches

# 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”

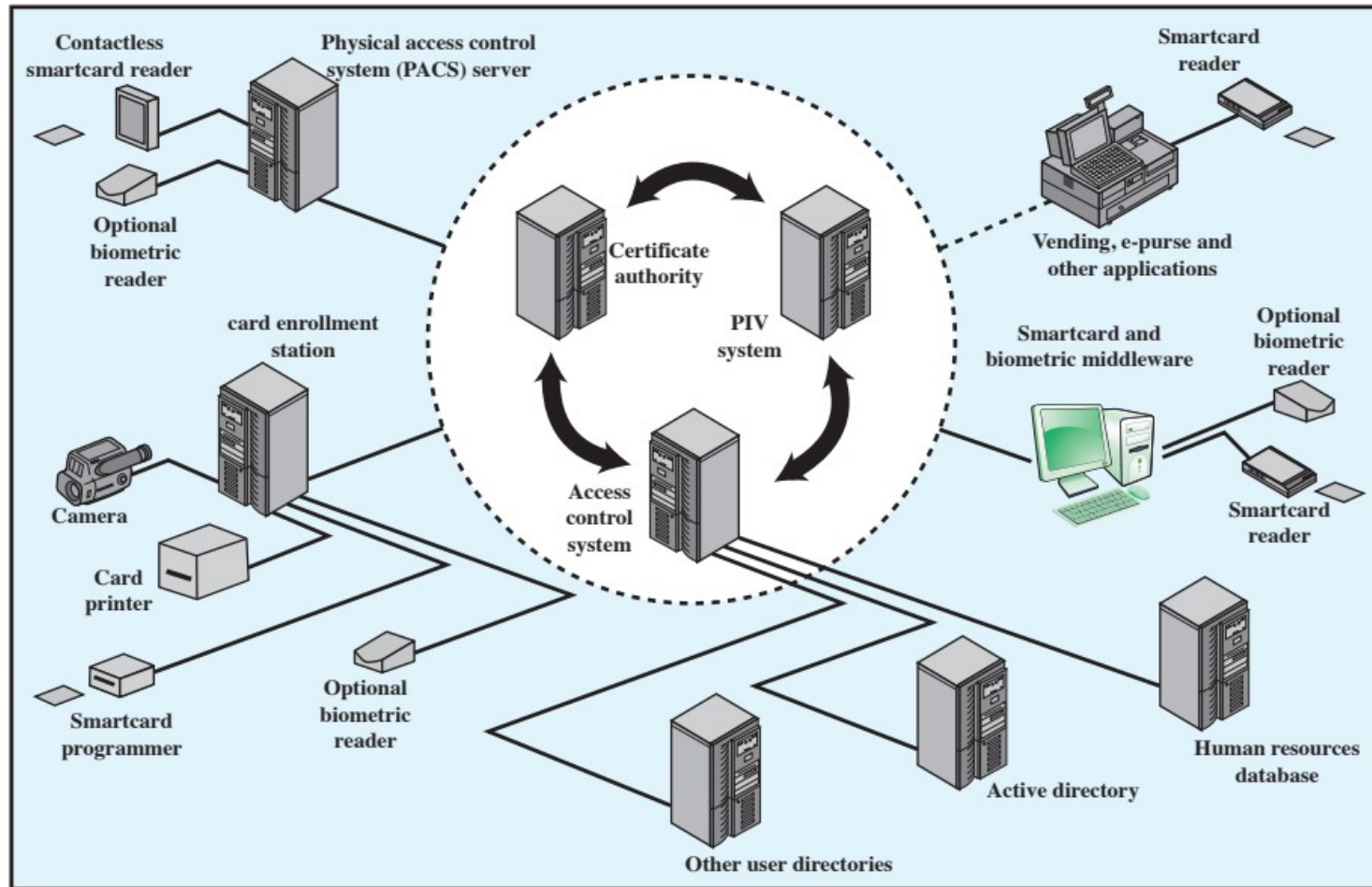


Figure 16.3 Convergence Example

# Convergence Example

# Degrees of Security and Control for Protected Areas

---

| 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.  |

# Chapter 17

## Human Resources Security



# Security Awareness, Training, and Education

---

The topic of security awareness, training, and education is mentioned prominently in a number of standards and standards-related documents, including ISO 27002 (Code of Practice for Information Security Management) and NIST SP 800-100 (Information Security Handbook: A Guide for Managers).

# Benefits to Organizations

---

Security awareness, training, and education programs provide four major benefits to organizations:

- Improving employee behavior
- Increasing employee accountability
- Mitigating liability for employee behavior
- Complying with regulations and contractual obligations

# Human Factors

---

**Employee behavior is a critical concern in ensuring the security of computer systems and information assets**



**Principal problems associated with employee behavior are:**

**Errors and omissions**

**Fraud**

**Actions by disgruntled  
employees**

|                         | <b>Awareness</b>  | <b>Training</b>  | <b>Education</b>   |
|-------------------------|---|--|--|
| <b>Attribute</b>        | "What"  | "How"  | "Why"  |
| <b>Level</b>            | Information   | Knowledge  | Insight  |
| <b>Objective</b>        | Recognition   | Skill  | Understanding  |
| <b>Teaching method</b>  | <b>Media</b><br>—Videos<br>—Newsletters<br>—Posters, etc. | <b>Practical instruction</b><br>—Lecture<br>—Case study workshop<br>—Hands-on practice | <b>Theoretical instruction</b><br>—Discussion seminar<br>—Background reading |
| <b>Test measure</b>     | True/false<br>Multiple choice<br>(identify learning)      | Problem solving<br>(apply learning)  | Essay<br>(interpret learning)  |
| <b>Impact timeframe</b> | Short term  | Intermediate   | Long term  |

# Comparative Framework

---

# Awareness

---

Seeks to inform and focus an employee's attention on security issues within the organization

- ▢ Aware of their responsibilities for maintaining security and the restrictions on their actions
- ▢ Users understand the importance of security for the well-being of the organization
- ▢ Promote enthusiasm and management buy-in
- ▢ Program must be tailored to the needs of the organization and target audience
- ▢ Must continually promote the security message to employees in a variety of ways
- ▢ Should provide a security awareness policy document to all employees

# Training

---

Designed to teach people the skills to perform their IT-related tasks more securely

- *What* people should do and *how* they should do it

General users

- Focus is on good computer security practices

Programmers, developers, system maintainers

- Develop a security mindset in the developer

Management-level

- How to make tradeoffs involving security risks, costs, benefits

Executive-level

- Risk management goals, measurement, leadership

# Employment Practices and Policies

---

Managing personnel with potential access is an essential part of information security

## Employee involvement:

- Unwittingly aid in the commission of a violation by failing to follow proper procedures
- Forgetting security considerations
- Not realizing that they are creating a vulnerability
- Knowingly violate controls or procedures

# Security in the Hiring Process

---

## Objective:

- “To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities”

## Need appropriate background checks and screening

- Investigate accuracy of details
- For highly sensitive positions:
- Have an investigation agency do a background check
- Criminal record and credit check



# Employment Agreements

---

Employees should agree to and sign the terms and conditions of their employment contract, which should include:

- I. Employee and organizational responsibilities for information security
- II. A confidentiality and non-disclosure agreement
- III. Reference to the organization's security policy
- IV. Acknowledgement that the employee has reviewed and agrees to abide by the policy

# During Employment

---

## Objectives with respect to current employees:

- Ensure that employees, contractors, and third-party users are aware of information security threats and concerns and their responsibilities and liabilities with regard to information security
- Are equipped to support the organizational security policy in their work
- Reduce the risk of human error

## Two essential elements of personnel security during employment are:

- A comprehensive security policy document
- An ongoing awareness and training program

## Security principles:

- Least privilege
- Separation of duties
- Limited reliance on key employees

# Termination of Employment

---

Termination security objectives:

- Ensure employees, contractors, and third party users exit organization or change employment in an orderly manner
- The return of all equipment and the removal of all access rights are completed

## Critical actions:

- Remove name from all authorized access lists
- Inform guards that ex-employee general access is not allowed
- Remove personal access codes, change physical locks and lock combinations, reprogram access card systems
- Recover all assets, including employee ID, portable USB storage devices, documents, and equipment
- Notify by memo or e-mail appropriate departments

# Email and Internet Use Policies

---

Organizations are incorporating specific e-mail and Internet use policies into their security policy document

Concerns for employers:

- Work time consumed in non-work-related activities
- Computer and communications resources may be consumed, compromising the mission that the IT resources are designed to support
- Risk of importing malware
- Possibility of harm, harassment, inappropriate online conduct

# Suggested Policies

---

**Business use  
only**

**Policy scope**

**Content  
ownership**

**Privacy**

**Standard of  
conduct**

**Reasonable  
personal use**

**Unlawful  
activity  
prohibited**

**Security  
policy**

**Company  
policy**


**Company  
rights**

**Disciplinary  
action**

# Security Incidents

---

**“Any action that threatens one or more of the classic security services of confidentiality, integrity, availability, accountability, authenticity, and reliability in a system”**



## **Unauthorized access to a system**

- Accessing information not authorized to see
- Passing information on to a person not authorized to see it
- Attempting to circumvent the access mechanisms
- Using another person's password and user id



## **Unauthorized modification of information on the system**

- Attempting to corrupt information that may be of value
- Attempting to modify information without authority
- Processing information in an unauthorized manner

# Detecting Incidents

---

Incidents may be detected by users or administration staff

- Staff should be encouraged to make reports of system malfunctions or anomalous behaviors
- Automated tools
- System integrity verification tools
- Log analysis tools
- Network and host intrusion detection systems (IDS)
- Intrusion prevention systems

# Triage Function

---

## Goal:

- Ensure that all information destined for the incident handling service is channeled through a single focal point
- Commonly achieved by advertising the triage function as the single point of contact for the whole incident handling service

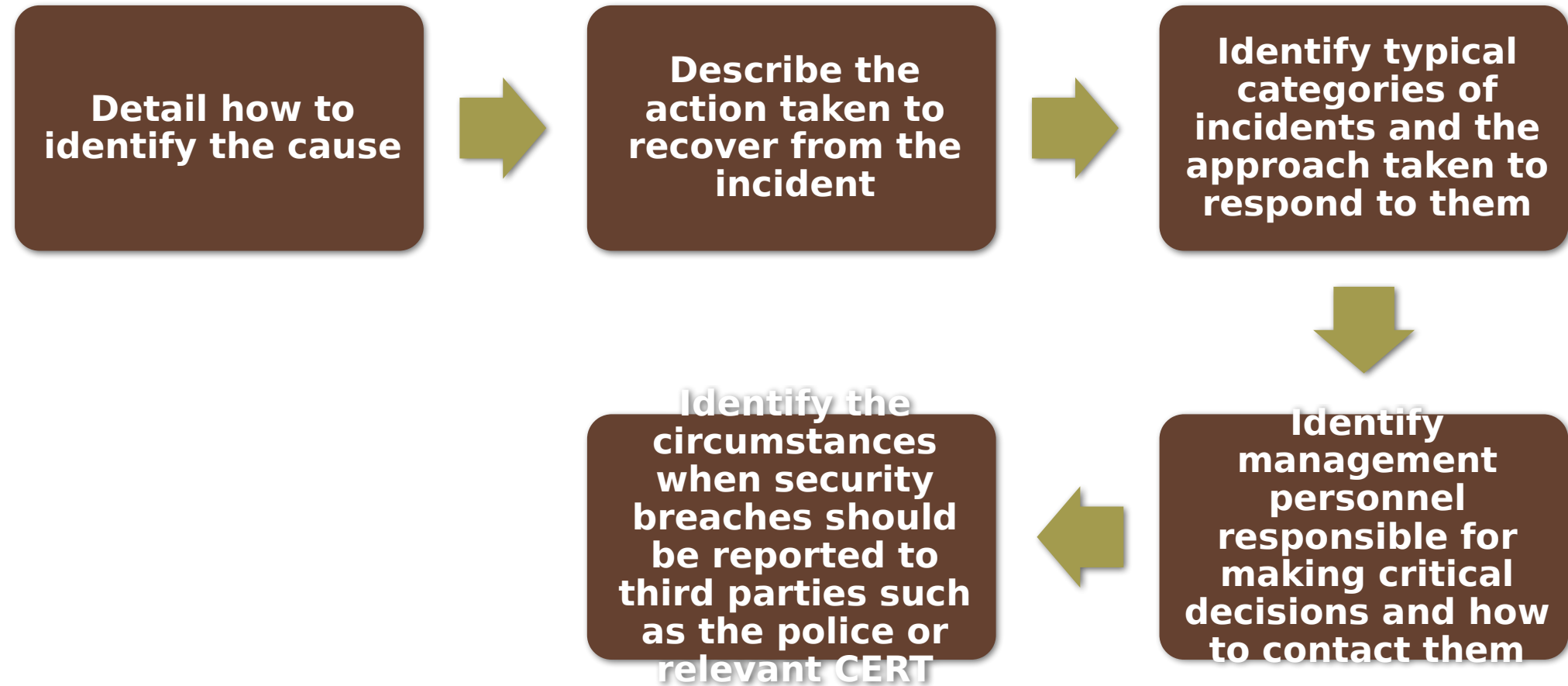
## Responds to incoming information by:

- Requesting additional information in order to categorize the incident
- Notifying the various parts of the enterprise or constituency about the vulnerability and shares information about how to fix or mitigate the vulnerability
- Identifies the incident as either new or part of an ongoing incident and passes this information on to the incident handling response function



# Responding to Incidents

---



# Documentation of Incidents

---

Should immediately follow a response to an incident

- Identify what vulnerability led to its occurrence
- How this might be addressed to prevent the incident in the future
- Details of the incident and the response taken
- Impact on the organization's systems and their risk profile