Unit-2
Physical Security Control & Operation Security

Physical Security Control

- Physical security deals with who has access to buildings, computer rooms, and the devices within them.
- Controlling physical security involves protecting sites from natural and man-made physical threats through proper location and by developing and implementing plans that secure devices from unauthorized physical contact.

Understanding the physical security domain

- The Physical Security domain includes the more traditional safeguards against threats, both intentional and unintentional, to the physical environment and the surrounding infrastructure.
  - How to choose a secure site (location) and guarantee the correct design
  - How to secure a site against unauthorized access
  - How to protect equipment, such as personal computers and the information contained on them, against theft
  - How to protect the people and property within an installation

Physical Security Threats

- The CBK defines these major categories of physical security threats:
- **Weather:** Tornadoes, hurricanes, floods, fire, snow, ice, heat, cold, humidity, and so forth
- • **Fire/chemical:** Explosions, toxic waste/gases, smoke, and fire
- • **Earth movement:** Earthquakes and mudslides
- • **Structural failure:** Building collapse because of snow/ice or moving objects (cars, trucks, airplanes, and so forth)
- • **Energy:** Loss of power, radiation, magnetic wave interference, and so forth
- • **Biological:** Virus, bacteria, and infestations of animals or insects
- • **Human:** Strikes, sabotage, terrorism, and war

Providing physical security

- There are five areas of providing physical security.
- Education for personnel
- Administrative access controls, such as work area restrictions, visitor control, and site selection
- Physical security controls, such as perimeter security controls, badging, keys and combination locks, security dogs, lighting, fencing, and guards
- Technical controls, such as smart cards, audit trails, intrusion detection systems, and biometrics
- Environmental/life safety controls

1. **Education for Personnel**

- An educated staff that knows about the potential for theft and misuse of facilities and equipment is the best weapon a company can have against illegitimate and accidental acts by others.
- Being mindful of physical and environmental considerations required to protect the computer systems
- Monitoring the unauthorized use of equipment and services, and reporting suspicious or unusual activity to security personnel
- Recognizing the security objectives of the organization
- Accepting individual responsibilities associated with their own security and that of their coworkers, as well as the equipment they use and how they use it

2. **Administrative Access Controls**

- The second category of physical access controls, administrative access controls, addresses the procedural and codified application of physical controls
- One of the administrative access controls in this section, site selection, involves planning for and designing the site before it is constructed.

2.1 Restricting Work Areas

- A physical security plan should first identify the access rights to the site (campus) in general and then identify the various access rights each location (building) within the site requires.
- Within a manufacturing plant, individuals might need different access privileges, based on the department or area they are attempting to enter, even though they have gained general admittance to the plant.
- A single mechanism can control various levels of security access.

2.2 *Visitor Control*

- Controlling visitor access to a building is not a new concern.
- Most companies have long had some kind of procedure for requiring visitors to sign in and specify a purpose for their visit, and then wait for an escort who authorizes their presence before granting access to the visitor.
- For less secure and nongovernment sites, visitors typically must have a clear purpose for their visit and a confirmed contact within the site, such as an employee or another individual with the appropriate clearance.
- In addition, visitors might be required to pass through a metal detector and should be prepared to have handbags, satchels, and laptop briefcases checked.
- They also should be ready to surrender, at least temporarily, recording devices such as cameras, tape recorders, and other questionable items (for example, pocketknives).

Registration

Regisited by OCR/ ID Reader

Pop-up Notification for New Visit

Once the visitors registered, he might be allowed to access all area of the office/ building

2.3 ***Site Selection***

- Site designers and planners must make at least the following considerations when deciding on the location for a facility.
- **Visibility:** How conspicuous will the facility be at a particular site? Most data centers look nondescript for a reason: They don't want to advertise what they are and attract undue attention. You will never find signs along the highway stating, "Highly Secure but Anonymous-Looking Data Operations Facility, Exit Here!" *Low-key* is the byword.
- • **Locale considerations:** A wise prospective homeowner should always inspect the neighborhood before purchasing a new house. The same rule applies to site-selection committees. What are the local ordinances and variances? What is the crime rate of the surrounding neighborhood? Are potentially hazardous sites nearby, such as landfills, hazardous waste dumps, or nuclear reactors?

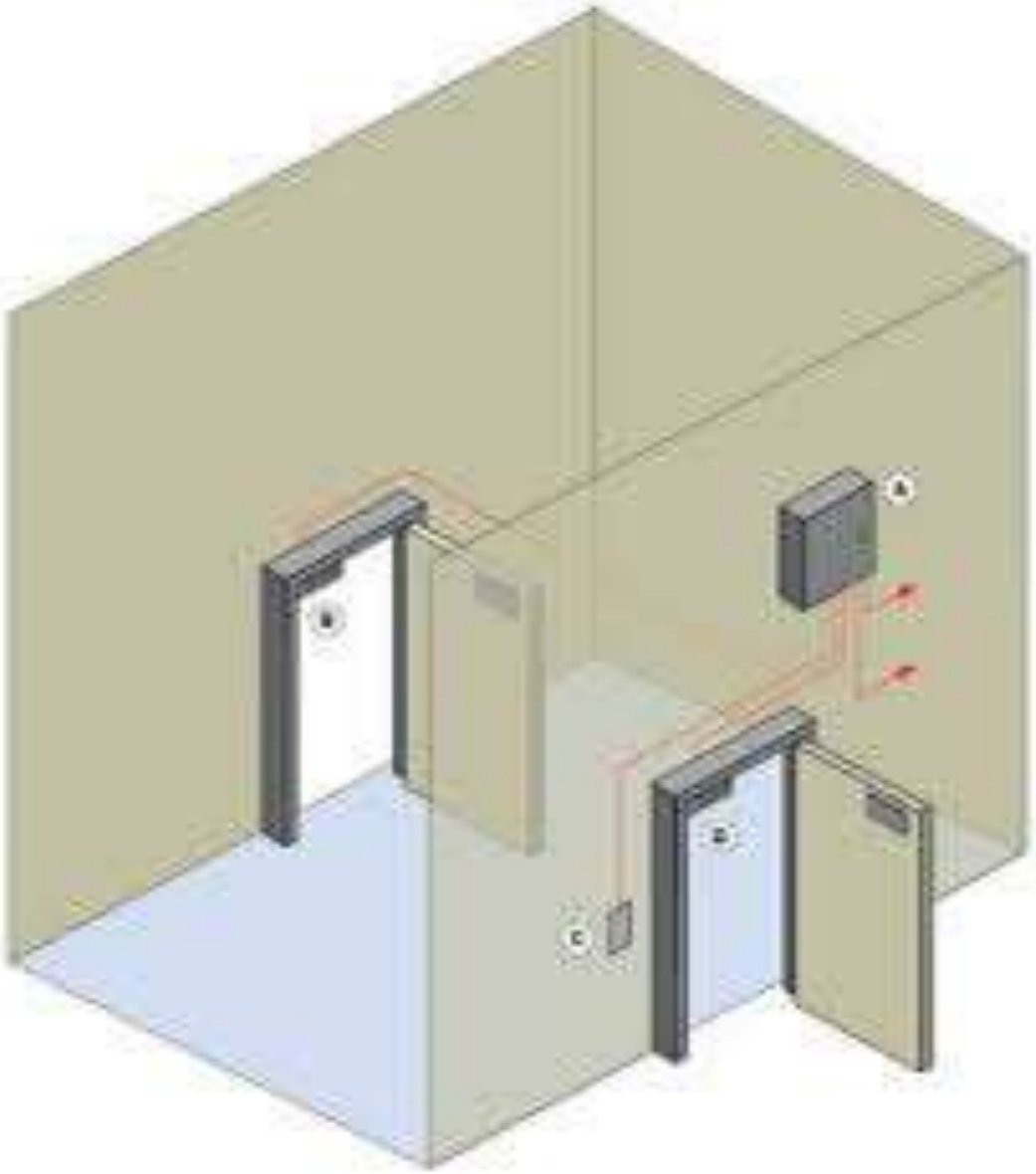
- **Natural disasters:** Several major corporations (including Charles Schwab) have moved their computer operations centers from the West Coast, particularly the San Francisco Bay area, to more geologically stable locations because of the risk of earthquakes. Other obvious natural threats to consider are tornadoes, hurricanes, floods, wildfires, chemical fires, vermin, pest damage, and snow and ice. Mother Nature's hand is far reaching, but site planners can minimize risk by examining local weather patterns, checking the history of weather-related disasters, and determining their risk tolerance.
- • **Transportation:** Are transportation routes such as airports, highways, and railroads nearby? If so, are they navigable? A good transportation system is important not only for the delivery of goods and services, but also for emergency evacuation procedures as part of a disaster recovery plan (DRP).

3. **Physical Security Controls**

- These include controls for the perimeter of the data center, employee and visitor badging, guard dogs when deemed appropriate, and building lighting.

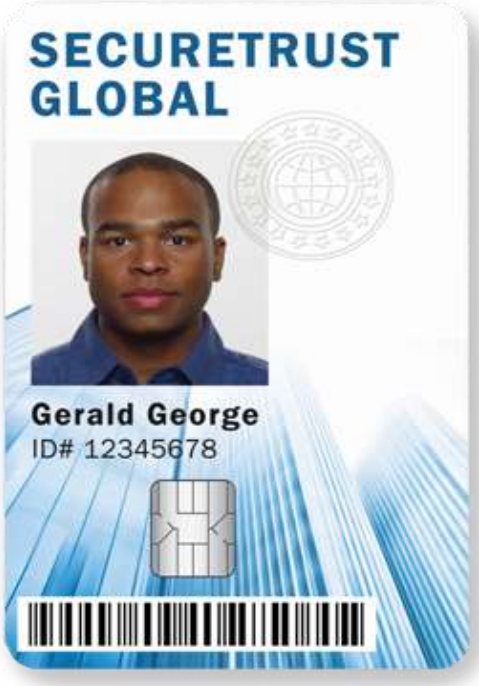
3.1 *Perimeter Security Controls*

- Controls on the perimeter of the data center are designed to prevent unauthorized access to the facility.
- For example, a gate might allow controlled access during the day but be locked or closed at night.
- Mantraps, as the name implies, are enclosed areas with a secure door on either end that literally “trap” an individual between doors.
- They address the problem of “piggybacking,” in which an individual without proper authorization enters a secure area behind an authorized person.
- To pass through the second door of the mantrap, the individual must pass a second level of validation—perhaps the authorization of a security guard, the entering of a password, or some other mechanism



3.2 ***Badging***

- Issued by a site security office, the photo identification badge is a perimeter security control mechanism that not only authenticates an individual, but also continues to identify the individual while inside the facility.
- Most sites issuing photo identification require that the individual display the badge where it is most visible, usually on the upper torso.
- The badge alone is no guarantee that unauthorized individuals are denied access—badges can be stolen and photos replaced—but combined with other perimeter controls, the badge offers a familiar and comfortable sense of security in most organizations.


SECURETRUST
GLOBAL
Gerald George
ID# 12345678

3.3 *Keys and Combination Locks*

- Keys and combination locks are how most people know physical security, mainly because they are the least complicated and expensive devices.
- Beyond the mechanical door lock opened with a key, locks can be programmed and opened with a combination of keys (such as the five-key pushbutton lock once popular in IT operations), a security badge with a magnetic strip, or some other mechanism.
- Locks are typically unguarded and are meant to delay intruders, not to deny them access.
- For that reason, you rarely find these devices in areas that require a high level of access authorization.

3.4 ***Security Dogs***

- Dogs are not just man's best friend—they also make great security guards.
- Dogs can be unflinchingly loyal and rely on all their senses to detect intruders.
- They can also be trained to perform specialized services, such as sniffing out drugs or explosives at airports or alerting the blind to fire.
- dogs are a highly effective form of perimeter security control when handled properly and humanely.

3.5 ***Lighting***

- Lighting is another form of perimeter protection that discourages intruders or other unauthorized individuals from entering restricted areas.
- many homeowners have motion-detector lights installed on garages and back porches.
- Critical buildings and installations should use some form of lighting as a deterrent, whether floodlights, streetlights, or searchlights.

4. Technical Controls

- The following are prominent technical controls:
- Smart/dumb cards
- Audit trails/access logs
- Intrusion detection
- Biometric access controls

4.1 ***Smart Cards***

- A smart card resembles a regular payment (credit) card, but it carries a semiconductor chip with logic and nonvolatile memory.
- the smart card has many purposes, including value for consumer purchases, medical identification, travel ticketing and identification, and building access control.
- The card can also store software that detects unauthorized tampering and intrusions to the chip itself and, if detected, can lock or destroy the contents of the chip to prevent disclosure or unauthorized uses.
- Smart cards can also facilitate file encryption by storing the user's private key.
- Still, smart cards alone are not completely secure. If an attacker steals a user's PIN or password along with the card, he or she gains complete access to the network. However, using a fingerprint along with the card to authenticate the user greatly reduces the chance for intrusion.

- The use of smart cards in conjunction with biometrics authentication, such as fingerprint readers or retinal scan techniques, can be extremely effective, especially when controlling physical access is of the utmost importance.

4.2 ***Audit Trails and Access Logs***

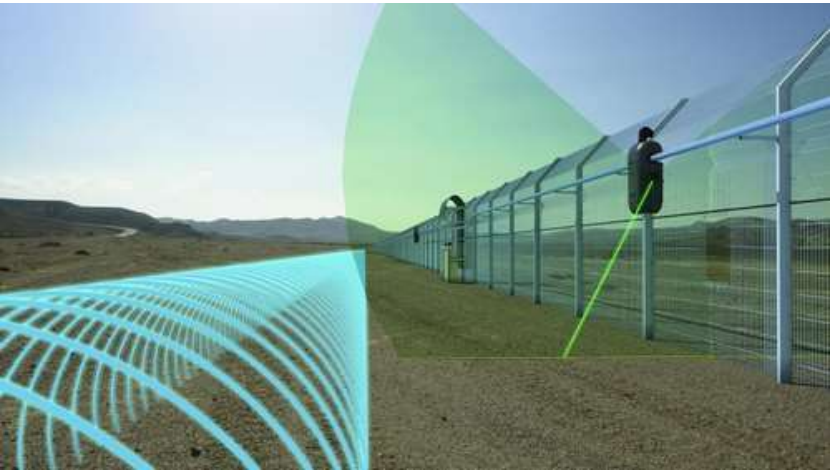
- In financial settings such as banks, audit trails enable examiners to trace or follow the history of a transaction through the institution.
- For example, bank auditors or examiners can determine when information was added, changed, or deleted within a system, to understand how an irregularity occurred and hopefully correct it.
- The audit trail should contain the following information:
- The user ID or name of the individual who performed the transaction
- Where the transaction was performed (hopefully using a fixed terminal ID)
- The time and date of the transaction
- A description of the transaction—that is, what function the user performed and on what device

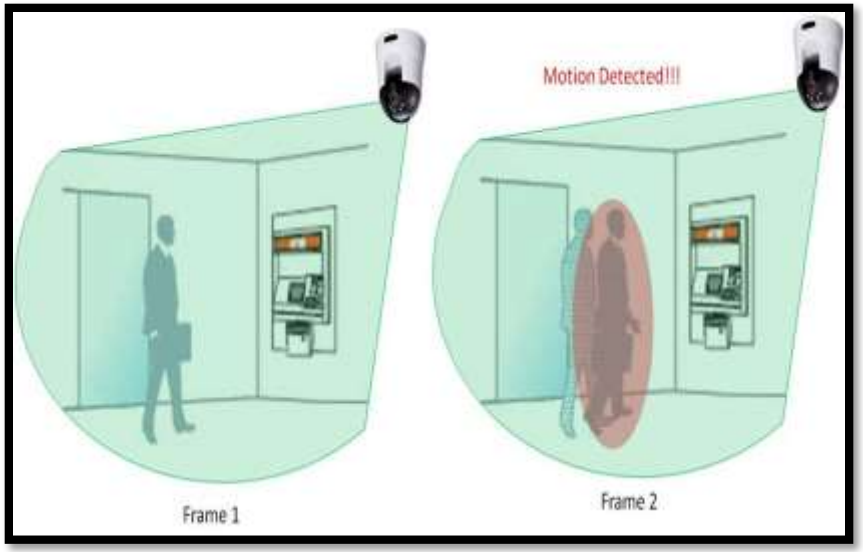
4.3 *Intrusion Detection*

- Intrusion detection is another type of technical control.
- . In this case, intrusion detectors and alarms alert security personnel when an unauthorized person attempts to access a system or building.
- The burglar alarm is the most commonly known intrusion detection device, but as you can imagine, the technology has become much more sophisticated since the first devices were used.
- Consider the two categories of devices:

- **Perimeter intrusion detectors:**
- These devices are based on dry contact switches or photoelectric sensors.
- The former consists of metallic foil tape placed on windows or doorframes using contact switches.
- Disturbing the switches sets off an alarm.
- Dry contact switches are used in residential homes and shop fronts, where cost is important.
- Photoelectric sensors receive light beams, typically infrared, from a light-emitting device.
- When an intruder breaks the beams of light, he or she trips an alarm.
- This type of intrusion detection device is more expensive and usually found in larger facilities.

- **Motion detectors:**
- These devices detect unusual movements within a well-defined interior space.
- Included in this category of intrusion detection devices are wave pattern detectors that detect changes to light-wave patterns and audio detectors that passively receive unusual sound waves and set off an alarm.





4.4 ***Alarm Systems***

- The implementation of a series of the aforementioned intrusion detectors is referred to as an alarm system.
- A local alarm system sets off an alarm on the premises, alerting guards.
- Private security firms manage central-station systems, such as home alarms from ADT and other well-known home security companies.
- They monitor a system 24 hours a day and respond to alerts from a central location.
- Dedicated systems might be more sophisticated than a local alarm system and share many of the same features as the centralized version.
- Additional alarms can be triggered at police or fire stations, with the permission and knowledge of the company being protected.

4.5 ***Biometrics***

- The use of biometrics in conjunction with more standard forms of authentication such as fixed passwords and PINs is beginning to attract attention as the cost of the technology decreases and its sophistication increases.
- Biometrics authentication uses characteristics of the human face, eyes, voice, fingerprints, hands, signature, and even body temperature; naturally, each technique has its strengths and weaknesses.
- Any security system, especially biometrics systems, must balance convenience with security.
- A system that is too intrusive or cumbersome will discourage or prevent an authorized user from accessing a system.

5. **Environmental/Life Safety Controls**

- The three most critical areas follow:
  - Power (electrical, diesel)
  - Fire detection and suppression
  - Heating, ventilation, and air conditioning (HVAC)

5.1 Power

- Whereas human beings can light candles when the power goes out, computers depend on an uninterrupted and regulated supply of power for constant voltage and current—computer equipment is highly sensitive to fluctuations in either voltage or current.
- most sites have backup power sources such as diesel generators, a kind of private energy source that kicks in when the primary power source is interrupted or inadequate.
- When the humidity is too high (normally, above 60 percent), condensation on computer parts can occur, resulting in lost efficiency.

5.2 *Fire Detection and Suppression*

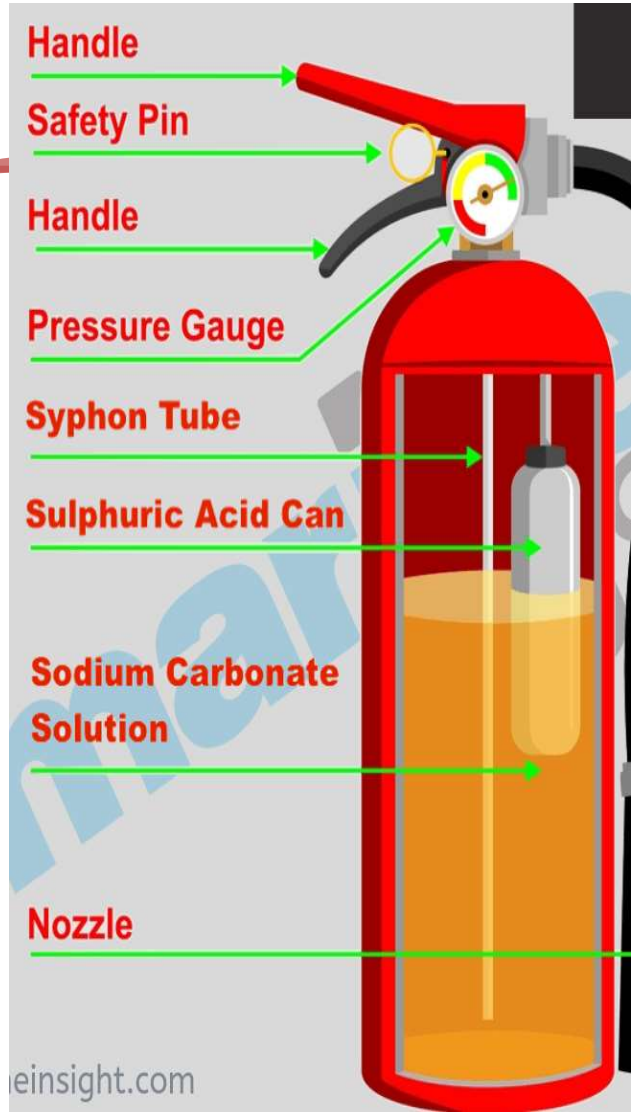
- It is outside the scope of this book to discuss at length the details surrounding this extremely important technical control.
- **Fire types:** Fires are classified according to the type of combustibles and recommended methods of suppression. The four types of fires include common combustibles (wood, paper, and so forth), liquids (petroleum products, coolants, and so forth), electrical, and combustible metal (such as magnesium).

- **Fire detectors:** Fire detectors can be one of several types. Heat-sensing systems respond to either a predetermined threshold or a rapid rise in temperature. Flame detectors sense infrared energy or the pulsation of the flame. Smoke detectors use photoelectric sensors to respond to variations in the light hitting the photoelectric cells.

- **Fire-extinguishing systems:** When a fire occurs, the heating, ventilation, and air conditioning system (HVAC) must be stopped immediately to prevent the flow of oxygen. To extinguish the fire, either a water-sprinkler system or a gas-discharge system is used.

- Water-sprinkler systems have four classifications: wet pipe, dry pipe, deluge, and preaction.
- Wet pipe systems hold water in the pipes that is released when heat opens a valve.
- Dry pipe systems do not have standing water in the pipes, so they eliminate the potential damage of a flood from a burst pipe in a wet pipe system. When water is needed, a central valve outside the data center is opened (automatically when a fire is sensed), and water flows into the plumbing only when it's required to extinguish a fire.
- The deluge system is a dry pipe system with a substantially higher volume of water.
- The preaction system combines elements of both wet and dry pipe systems and is the recommended fire-extinguishing system for computer rooms.

- Gas Discharge System:
- Carbon dioxide is another commonly used gas in fire suppression systems. Like clean agents, carbon dioxide does not require clean up after discharge. Unlike clean agents, carbon dioxide puts out fires by removing oxygen, not heat. This is a critical difference, because it means that carbon dioxide can not be used in occupied spaces.
- Because carbon dioxide removes oxygen, it can suffocate people. If you are using a carbon dioxide system for fire suppression, make sure to completely ventilate the area if the system goes off. Only then is it safe for personnel to assess the damage.



5.3 *Heating, Ventilation, and Air Conditioning (HVAC)*

- The classifieds always seem to have ads for HVAC repairmen.
- That's because reliable and uninterrupted heating, ventilation, and air conditioning systems are critical environmental controls.
- Computers are particularly sensitive to the smallest fluctuations in temperature and humidity.
- We frequently take HVAC environmental controls for granted, but the IT manager or the person(s) responsible for these systems should know exactly what to do and whom to contact in the event of failure.
- Routine maintenance of critical infrastructure systems should prevent any significant failure of HVAC systems.

Operation Security

- Operations security is used to identify the controls over software, hardware, media, and the operators and administrators who possess elevated access privileges to any of these resources.
- Operations security is primarily concerned with data center operations processes, personnel, and technology, and is needed to protect assets from threats during normal use.

OPERATIONS SECURITY PRINCIPLES

- The principle of least privilege, or need to know, defines a minimum set of access rights or privileges needed to perform a specific job description.
- For example, a system administrator should have the necessary privileges to install server operating systems and software but should not have the role to add new users to the server.
- of duties is a type of control that shows up in most security processes to make certain that no single person has excessive privileges that could be used to conduct hard-to-detect business fraud or steal secrets from a government system.
- Separation of duties is one of the six key elements of a strong system of security controls.

- These six elements are listed here:
- Employing competent, trustworthy people with clear lines of authority and responsibility
- Having adequate separation of job and process duties
- Having proper procedures for authorizing transactions or changes to information
- Maintaining adequate documents and records
- Maintaining appropriate physical controls over assets and records
- Executing independent checks on performance

- A primary benefit of separation of duties is that it enables one person's work to serve as a complementary check on another person's work.
- This implies that no single person has complete control over any transaction or process from beginning to end.
- Separation of duties is important within all security-related processes for two fundamental reasons.
- First, people are an integral part of every operations process.
- Second, people have shortcomings.
- In spite of these checks and balances, some people might still be inclined to engage in fraud, theft, or malicious activities. They usually do so because they possess the following:

- **Motivation:** Usually caused by some financial crisis that results from health problems, drugs, overspending, gambling, extortion, or relationship problems, for example.
- • **Justification:** A sense that they have not been treated fairly, the employer owes them, or any other explanation that they use to give good reason for their actions
- • **Opportunity:** Knowledge or belief that a fraud can be committed and remain undetected (“I’ll never get caught”) either because internal controls are not in place or are inadequate, or because they believe no one is minding the store.

OPERATIONS SECURITY PROCESS CONTROLS

- Process controls are necessary for secure data center operations.
- They help ensure that the principles outlined previously are implemented in human-based process activities and software-based utilities and other data center management systems (such as backup libraries and program directories).
- 1. Trusted recovery controls
- It ensures that security is not breached when a computer system crashes.
- One example of this is a bank vault located in a high-security room. The trusted recovery control is the room itself, which can detect any attempt at an unauthorized entry and lock the perpetrator in an area where he cannot escape

- 2. Configuration and change management controls
- They are used for tracking and approving changes to a system.
- This process identifies, controls, and audits any changes by administrative personnel to reduce the threats or negative impacts of security violations.
- One threat to configuration and change management is called a block upgrade.
- In this situation, a requestor asks for a large number of simultaneous changes during an upgrade, but because change management is impossible, it is bypassed.
- 3. Personnel security
- It involves pre-employment screening and mandatory vacation time.
- This prevents people from hiding illegal activities while performing their duties.
- Other personnel security measures include job rotation and a series of escalating warnings that lead up to termination of employment or prosecution in the criminal justice system in cases of unauthorized or illegal activity.

- 4. Record retention processes
- It refers to how long transactions and other types of computerized or process records should be retained.
- These controls deal with computer files, directories, and libraries of software and utilities.
- 5. Resource protection
- It is needed to protect company resources and assets.
- Some resources that require protection are modem pools, network routers, storage media, and documentation.
- 6. Privileged entity controls
- They are given to operators and system administrators as special access to computing resources.
- 7. Media viability controls
- They are needed for the properly marking and handling assets.
- These include clearly marking media with contents, dates, classification (if needed), and other information to help operators locate and use the correct media more often.
- 8. Operations process controls
- They are a necessary element in the overall security of a computer installation.

OPERATIONS SECURITY CONTROLS IN ACTION

- Following section provides more details on specific areas of operations used as protection against this vulnerability.
- To ensure operations security, the individuals in charge of information security must keep these considerations in mind at all times:
- • Software support
- • Configuration and change management
- • Backups
- • Media controls
- • Documentation
- • Maintenance
- • Interdependencies

- A. ***Software Support :***
- Software is the heart of an organization's computer operations, regardless of the size and complexity of the system.
- One type of control within this category is to limit what software is used on a given system.
- A second method of controlling software is to inspect or test software before it is loaded
- In addition to controlling the loading and execution of new software, organizations should be cautious with off-the-shelf or downloaded system utilities.
- Another element of software support involves ensuring that software is not modified without proper authorization.
- This involves protecting all software and backup copies.

- B. ***Configuration and Change Management***
- Configuration and change management, which is closely related to software support, tracks and, if needed, approves changes to the system.
- The primary security goal of configuration management is ensuring that users don't cause unintentional changes to the system that could diminish security.
- A second security goal of configuration and change management is to ensure that changes to the system are reflected in up-to-date documentation.
- If the change is major, it might be necessary to reanalyze some or all of the system's security.

- C. ***Backups***
- Support and operations personnel (and sometimes users) back up software and data.
- The frequency of backups depends on how often data changes and the importance of those changes.
- backups should be stored securely and off site.
- Users of smaller systems are often responsible for their own backups.
- However, they do not always perform backups regularly or thoroughly.
- In some organizations, support personnel are charged with making backups periodically for smaller systems, either automatically (through server software) or manually (by visiting each machine).

- D. ***Media Controls***
- Media controls include a variety of measures to provide physical and environmental protection and accountability for tapes, diskettes, optical media, USB (Flash) drives, printouts, and other media.
- media controls should be designed to prevent the loss of confidentiality, integrity, or availability of information, including data or software, when stored outside the system.
- The extent of media control depends on many factors, including the type of data, the quantity of media, and the nature of the user environment.
- The next sections describe some of the common media controls.

- **Marking**
- Controlling media might require some form of marking or physical labeling.
- The labels can be identify media with special handling instructions, locate needed information, or log media (for example, with serial/control numbers or bar codes) to support accountability.
- Colored labels often identify media, and banner pages are used on printouts.
- marking backup media can help prevent them from being accidentally overwritten.
- **Logging**
- Logs can include control numbers (or other tracking data), the times and dates of transfers, names and signatures of individuals involved, and other relevant information.
- Automated media tracking systems are helpful in maintaining inventories of media libraries.

- **Integrity Verification**
- When electronically stored information is read into a computer system, you might need to determine whether it has been read correctly or subjected to any modification.
- You can verify the integrity of electronic information using error detection and correction or, if intentional modifications are a threat, cryptographic-based technologies.
- In addition, the integrity of backup media should be tested periodically so that no surprises arise when it's time to rely on them to restore normal operations.
- **Physical Access Protection**
- Media can be stolen, destroyed, replaced with a look-alike copy, or lost.
- Physical access controls that limit these problems include locked doors, desks, file cabinets, and safes.
- If the media requires protection at all times, it may be necessary to actually output data to the media in a secure location.
- protection of media should extend to backup copies stored offsite.

- **Environmental Protection**
- Magnetic media, such as CDs, DVDs, and other optical media, require environmental protection because they are sensitive to temperature, liquids, magnetism, smoke, and dust.
- Other media, such as paper and other storage, have different sensitivities to environmental factors.
- **Transmittal**
- Media control can be transferred both within the organization and to outside elements.
- Possibilities for securing such transmittal include sealed and marked envelopes, authorized messenger or courier.

- **Disposition**
- When media is disposed of, it might be important to ensure that information is not improperly disclosed.
- People often throw away old media, believing that erasing the files has made the data irretrievable.
- Commonly available utility programs can easily retrieve information that is presumed deleted.
- To prevent the threats from recovering information from disposed media, we turn to the technique of permanently removing information from media, called sanitization.
- Three techniques are commonly used for media sanitization:
- • Overwriting : Overwriting is an effective method for clearing data from magnetic media. As the name implies, overwriting uses a program to write data (1s, 0s, or a combination) onto the media.
- • Degaussing : Degaussing involves magnetically erasing data from magnetic media. Two types of degaussers exist: strong permanent magnets and electric degaussers.
- • Destruction : It is done by shredding or burning media.

- E. ***Documentation***
- The security of a system also needs to be documented.
- This includes many types of documentation, such as security plans, contingency plans, risk analyses, and security policies and procedures.
- Security documentation should be designed to fulfill the needs of the different types of people who use it.
- security procedures manual for systems operations and support staff can address a wide variety of technical and operational concerns in considerable detail.
- F. ***Maintenance***
- System maintenance requires either physical or logical access to the system.
- Maintenance can performed onsite, or you might have to move equipment to a repair site.
- Maintenance can also be performed remotely via communications connections.
- If someone who does not normally have access to the system performs maintenance, security vulnerability is introduced.

- G. ***Interdependencies***
- Support and operations components coexist in most computer security controls:
- **Personnel:** Most support and operations staff have special access to the system. Some organizations conduct background checks on individuals who fill these positions, to screen out possibly untrustworthy individuals.
- • **Incident handling:** Support and operations can include an organization's incident-handling staff. Even if they are separate organizations, they need to work together to recognize and respond to incidents.
- • **Contingency planning:** Support and operations normally provide technical input to contingency planning and carry out the activities of making backups, updating documentation, and practicing responses to contingencies.

- • **Security awareness, training, and education:** Support and operations staff should be trained in security procedures and be aware of the importance of security. In addition, they provide technical expertise needed to teach users how to secure their systems .
- • **Physical and environmental:** Support and operations staff often control the immediate physical area around the computer system .
- • **Technical controls:** Support and operations staff installs, maintains, and uses the technical controls. They create the user accounts, add users to access control lists, review audit logs for unusual activity, control bulk encryption over telecommunications links, and perform the countless operational tasks needed to use technical controls effectively.
- • **Assurance:** Support and operations staff ensures that changes to a system do not introduce security vulnerabilities by using assurance methods to evaluate or test the changes and their effect on the system.

Questions

1. What is physical security? List and explain its threats.
2. Explain areas providing physical security.
3. Write a short note on site selection.
4. Explain technical controls to provide physical security.
5. Write a short note on environmental and safety control.
6. Explain physical security controls in detail.
7. Explain operation security process controls.
8. Explain Operations security controls in action.
9. Explain media controls in operation security.
10. Write a short note on interdependencies.