Faculty of Computer Applications &
Information Technology

BCA Programme

210301502

INFORMATION SECURITY

Unit -2 Physical and Operations Security

- **Physical Security**
  - Introduction
  - Understanding the Physical Security Domain
  - Physical Security Threats
  - Providing Physical Security
- **Operation Security**
  - Introduction
  - Operations Security Principles
  - Operations Security Process Controls In Action

Unit -2 Physical Security

- **Introduction**
  - We must overlooked connection between **Physical System** (Computer hardware) and **Logical systems** (software) in order to protect logical systems.
  - **If we can't protect our hardware, we can't protect the programs and data** running on hardware.
  - Physical Security Deals with
    - Building
    - Computer Rooms
    - Devices etc...
  - Physical security **involves protecting site from natural and man made physical threats through proper plan that secure devices** from unauthorized physical contact.

Unit -2 Physical Security

- **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.
  - Example – Entry procedure for Government / Private Company
  - The **level of physical security** is typically **proportional to the the value of the property** that is being protected.
  - High level research generally use more sophisticated physical security checks, including biometrics as the primary level.

Unit -2 Physical Security

- Following areas need to understand to implement physical security.
  - **How to choose a secure site (location) and guarantee the correct design ?**
  - **How to secure a site against unauthorized access?**
  - **How to protect equipment against theft ?**
  - **How to protect the people and property within an installation ?**

Unit -2 Physical Security Threats

- The major categories of physical security threats, as defined in the CBK (Common Body of Knowledge) are:

(1) Weather

  - Tarnadoes, hurricanes, floods, fire, snow, ice, heat, cold, humidity and so forth....

(2) Fire / Chemical

  - Explosion, toxic waste/gases, smoke, fire.

(3) Earth Movement

  - EarthQuakes, mudslides

Unit -2 Physical Security Threats

- The major categories of physical security threats, as defined in the CBK (Common Body of Knowledge) are:

(4) Structural Failure

- Building collapse due to moveing objects (car, planes, trucks) or natural objects (snow, ice, flood)

(5) Energy

- Loss of power, radiation, magnetic wave interference ....

(6) Biological

- Virus, bacteria, infestations of animals ect...

(7) Human

- Strikes, sabotage, terrorism, war .....

Unit -2 Providing Physical Security

- Five areas of physical security that address the aforementioned types of physical security threats:

(1) Educating Personnel

(2) Administrative controls

(3) Physical controls

(4) Technical Controls

(5) Environmental / life safety controls

Unit -2 Providing Physical Security

(1) Educating Personnel

- An **educated staff, made aware of the potential for theft and misuse** of facilities and equipment.
- **Employees should be reminded periodically of the importance** of helping to secure their surroundings including:
  - Physical & environmental consideration to protect computer systems.
  - Emergency & disaster plans
  - Monitoring unauthorized use of equipments
  - Reporting unusual & suspicious activity
  - Recognizing security objectives.
- An **organization can educate its staff on the importance of their physica security** through the use of self – paced or formal instruction, bulletins, posters, training films or awareness days.

Unit -2 Providing Physical Security

(2) Administrative Access Controls

- **Administrator access controls, addresses the procedural and codified application of physical controls.**
- **Restricting Work Area**
  - A physical security plan – identify the access rights to the site
- **Escort Requirements and Visitor Control**
  - Company have long had some kind of procedure for requiring visitors t**o "sign in" and specify a purpose for their visit and wait for an escort** that authorizes their presence before granting access to the visitors.

Unit -2 Providing Physical Security

- **Site Selection**
  - **Site designers and planners must make at tleast the following considerations when deciding on the location for a facility.**
    - **Visibility**
    - **Locale considerations**
    - **Natural Disasters**
    - **Transportation**

Unit -2 Providing Physical Security

(4) Technical Controls

- **The more prominent technical controls include**
  - Smart / dumb cards
  - Audit trails / access logs
  - Intrusion detection
    - Perimeter instrusion Detectors
    - Motion Detectors
  - Biometric access conrtrols

Unit -2 Providing Physical Security

(5) Environmental / Life-Safety Controls

- **The more prominent technical controls include**
  - Power
  - Fire Detection and Suppression
  - Heating, Ventilation and Air Conditioning

Unit -2 Operations Security

- **Introduction**
  - 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.
  - Specific **types of controls are needed to implement** the security necessary to protect assets.
    - **Preventative controls**
      - reduce the frequency and impact of error and prevent unauthorized intruders.
    - **Detective Controls**
      - Discover errors once they have occurred.

Unit -2 Operations Security

- **Introduction**
  - **Specific types of controls are needed to impement the security necessary to protect assets.**
    - **Corrective or Recovery controls**
      - Help mitigate the impact of a loss.
    - **Deterrent Controls**
      - Encourage compliance with external controls.
      - *A deterrent control is anything intended to warn a would-be attacker that they should not attack. This could be a posted warning notice*

Unit -2 Operations Security

- **Introduction**
  - **Specific types of controls are needed to impement the security necessary to protect assets.**
    - **Application – level controls**
      - Minimize and detect software operational irregularities.
    - **Transaction – level controls**
      - Provide control over various stages of a transaction.

Unit -2 Operations Security

- 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.
- **Separation 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.**

Unit -2 Operations Security

- **Separation of duties** is one of the six key elements of a strong system of internal and security controls.

  (1) Employing competent, trustworthy people with clear lines of authority and responsibility.

  (2) Having adequate separation of job and process duties.

  (3) Having proper procedures for authorizing transactions or changes to information.

  (4) Maintaining adequate documents and records.

  (5) Maintaining appropriate physical controls over assets and records.

  (6) Executing independent checks on performance.

Unit -2 Operations Security

- **Separation of duties** (benefits)
  - It enables one **person's work to server as a complementary check on another person's work.**
  - This implies that **no one person has complete control over any transaction or process from beginning to end.**

Unit -2 Operations Security

- To ensure operation security, the individuals in charge of information security must keep a number of things in mind at all times. There are :
  - Software Support
  - Configuration and change management
  - Backups
  - Media controls
  - Documentation
  - Maintenance
  - Interdependencies

Unit -2 Operations Security

- **Software Support**
  - Software is the heart of an organization's computer operations.
  - Several elements of control are needed for software support:
    (1) Limiting what software is used on a given system.
    (2) Inspect or test software before it is loaded (This applies to new software, upgrades, off-the-shelf product etc.)
    (3) Software is properly licensed.
    (4) To assure that software is not modified without proper authorization.

Unit -2 Operations Security

- **Media Controls**
  - Media controls include a variety of measures to provide physical and environmental protection and accountability for tapes, diskettes, CD's, Zip etc.
  - Extent of media control depends on many factors, including the type of data, the quantity of media, and the nature of the user environment.
  - Some of the common media controls are described in the sections below:
    - Marking
    - Logging
    - Integrity Verification
    - Physical Access Protection
    - Environmental Protection
    - Transmittal
    - Disposition

Unit -2 Operations Security

- **Marking - Media Controls**
  - Controlling media may require some form of marking or physical labeling.
  - The label can be used to identify media with special handling instructions, locate needed information or log media to support accountability.
- **Logging - Media Controls**
  - Logging media supports **accountability**.
  - Logs can **include control numbers, the times and dates of transfers, names and signatures** of individuals involved.

Unit -2 Operations Security

- **Integrity Verification - Media Controls**
  - When electronically stored information is read into a computer system, it may be necessary to determine whether it has been read correctly or subject to any modification.
  - The integrity of electronic information can be verified using error detection ad correction.
- **Physical Access Protection - Media Controls**
  - Media can be stolen, destroyed, replaced with look-alike copy or lost.
  - So need to locked door, desk, cabinets etc.
  - Physical protection of media **should be extended to backup copies** stored offsite.

Unit -2 Operations Security

- **Environmental Protection - Media Controls**
  - Magnetic media required environmental protection, because they are sensitive to temperature, liquids, magnetism etc.
- **Transmittal - Media Controls**
  - Media control may be transferred both within the organization and outside elements.
  - Possibilities for **securing such transmittal include sealed and marked envelopes, authorized messenger or courier.**

Unit -2 Operations Security

- **Disposition - Media Controls**
  - **When media is disposed of, it may be important to ensure that information is not improperly disclosed.**
  - The technique of permanently removing information from media, called **sanitization.**
  - **Overwritting**
  - **Degaussing**
    - Is a method to magnetically erase data from magnetic media.
  - **Destruction**

Unit -2 Operations Security

- **Documentation**
  - Security of a system also need to be documented.
  - This includes many types of documentation:
    - Security plans
    - Contigency plans
    - Risk analyses
    - Security policies and procedures
- **Maintenance**
  - System maintenance requires either physical or logical access to the system.
  - **One of the most common methods that hackers use to break into systems is through maintenance accounts.**

Unit -2 Operations Security

- **Interdependencies**
  - Supports and operations components coexist in most computer security controls. These components are:
    - Personnel
    - Incident Handling
    - Contingency planning
    - Security awareness, training and education
    - Physical and environmental
    - Technical controls
    - Assurance