Information Security and Network Security

Chapter – 1

Introduction to Information Security

Components of information

1. Software
   like Brain of human body.

– H/W functioned by S/W- A program step by step instructions.
– It collects data, organizes and carries procedures
– Types of Software

- System software- enables the application S/W to interact with the comp H/W. It is collection of programs. In include. OSs, utilities and Device drivers and Compilers.
- Application S/W-end-user S/W
- General purpose- Browser, WS, DBMS & Excel[1]
- Special application-Graphics
- Customized s/w
- Mobile apps
- Readymade software

2. Hardware -physical component-All tangible equipment's e.g. computer set, printer , UPS, servers, CD/DVD, external HDD, camera, audio devices, Laptop, tabs, Smart phone, super computers, pen drive , secondary storage & discs.
3. Data - Heart of the S/W

– S/W cannot function without Data
– Qualitative and quantitative data
– It's Raw unprocessed facts

Types of data

– Documents files – Memos, term paper letters
– Worksheet Files-XLSX
– Database files – Created by DBMS- structured and organized
– presentation-files.PPT processed. Data yields information

4. People

– Important part of information
– Develop S/W and run it
– Enter the data

[1]

- Determines the success or failure of system
- It is easy to overlook people as one of the parts of information system

  System Analyst Developer, H/W Engg, System administrator, DBA, Operational user, End users, Management persons, S/W tester and Deployment Engg are the roles of peoples.

5.Proceehires-

Rules, instructions and descriptions how things are done. The rules or guidelines which are to be followed by people when working on S/W and data are known as procedures.

- Documentation in manuals written by computer specialists

6.Network and Internet

The connect device/hardware of information system.

- Internet: Almost all in information system connect and interact with other people and computers.

  Modem, switches, Cat6 cables, RJ45 Connectors, optic fiber cable

  N/W cards, Router etc.

Components of Information Security

Organization must learn to avoid pitfalls by protecting business information and keeping consumers' confidence organization must -

- Identify technology risks
- Analyze risks And
- Prepare for action plan

Components of information security are as follows

1) Information Security Risk Management
- Identify and manage the potential risk associated with information and IT in cost effective way.

  Information Security risk management practice applicable to-

- Employees , who are responsible for planning, analyzing, implementing and maintaining information security within organization.
- Employees and managers who are accountable for maintaining information security within organization.

2. Information Security Awareness
- Gap between the organization's operational requirements and technological requirements
- Employees no clear understanding of the organization's mission or sufficient knowledge about technology.
- Need training to employees about the importance of safe guarding information assets.

- Educate employees about the threats to the information assets of an organization.
- Training should be imparted to employees about safe downloads and other technology related issues.

3. Information Security Policies

- Defining information security polices
- Decide ‘baseline’ standards i.e. policies and rules
- A policy is a clear, Well-defined principle to which an action must be confirm.
- Policy is consistent with organizations strategic, mission. goals and objective when we define a policy that caters to information and technology needs, it is called an information security policy.

Information security policies help to:

- Identify and categorize the type of information and the level of protection the information needs.
- Identify the individuals who have access to information and define the type of access each employee is allowed.
- Define the use of proper authentication procedures.
- Inclement procedures to protect computer system from viruses.

Common policies every organization defines is the current usage of information resources. e.g. An employee can download any software application of net documentation from the internet only if –

The software, application or documentation is required for the current project the employee in assigned to

The employee has taken prior permission to download the software application or documentation from the concerned authority.

Punishment under the organization’s authorized us. Use of resources policy.

4. Information Security Design

Involves the planning and implementation of various software tools and technologies such as

- Firewalls
- Antivirus software
- Digital certificates - is a file or electronic password that proves the authenticity of device, Server or user through the use of cryptography and public key infrastructure. Digital certificate authentication helps organization on sure that only trusted devices and users can connect to their networks. It’s like identification card.
- Verification techniques - To protect information assets and network resources form harm.

Physical security

Need for physical security

- To avoid damage computer installations and data centers or computer networks.
- Can arise from natural disaster. e.g. fire, earth quakes floods etc.
- Disaster Recovery (DR) falls under physical security
- Physical Protection of information systems resources
- Well – protected IS needs 'Defense in depth' it means combining multiple security measures in order to make unauthorized in access difficult for an external intruder or even an employee who does not need to know.

What in physical security?

- Protects facility housing (information) systems resources themselves and the facilities used support their operation.
- Cover areas at a minimum access controls, fire safety, failure of supporting utilities structural collapse interception of data and mobile and portable systems.
- Protection of building sites, equipment from theft, vandalism, natural disaster manmade catastrophes (sudden damage) and accidental damage.
- Require solid building construction, suitable emergency preparedness, adequate climate control and appropriate protection from intruders (a person with criminal intent).
- Access control- Rules and department mechanism that control access IS and physical access to premises.

Natural disaster and controls

Digital equipment's are sensitive to many environmental factors

1. Fire- Affects Information system., major/minor.
   - To control install fire detectors near equipment.
   - Keep fire extinguisher near equipment and train employees in their proper use and conduct regular fire evacuation exercises- physical backup at other location.
2. Environmental failure
   - Interruption in supply of controlled environmental support
   - Clean air, air conditioning, humidity and water controls.
3. Earthquake- keep computer systems away from glass and elevated surface controls with anti-vibrations devices.
4. Liquid leakage / floods-
   - Burst or leaking pipes and accidental discharge of sprinklers.
   - keep liquid proof covers near the equipment.
   - Install water detectors on the at floor near computer systems.
   - flood level / in time precaution.
5. Lightning- An electric charge of air.

- Can cause either direct lightning strikes to the facility or surges thing to strikes to electric power transmission lines, transformers and substations.
- Install surge suppressors, store backups in grounded storage media and install UPS.

6. Electric Interruption
   - Disruption in electric power supply; longer than 30 min can have a serious business impact.
   - Install and test UPS.
   - Install line filters to control voltage strikes.
   - Install anti-static carpeting

Basic Principles of Physical Security of Information System

1.Defense-in-Depth

- Deploying multiple measures that complement and support one another to control
- Information system security procedures
- Physical space
- Personnel

Physical security measures must be designed to meet threat to security posed by the ill-intentional person. “trust no one’s”.

Precautions may include:

- Security key and contains to protect classified information
- Security alarm systems to default unauthorized access and alert a response
- Physical access control measures.
- Physical barriers to detect and delay unauthorized entry.

2. Controlling the Physical Access

The no of physical access/ entry points at facilities information, processing facilitie or data storage should be controlled.

- security doors
- shutters
- grills
- window bars.
- Closed Circuit Televisions Systems (CCTV)
- Guard Services

3. Intrusion Detection System (IDS)

Designed to detect or attempted unauthorized entry, identify its location and signal a response with an alarm.

IDS can:

- Provide continuous surveillance over secure areas.
- Extend coverage into areas not usually accessible to guards

4.Physical access on a need to know basis

- Access to information system resources must always be provided only on a need–to-know basis, potentially any one can be preparator/procedural and personnel measures.

-the need–to–know limiting access to official information to people who require it to carry out their duties.

- Identify material that needs special protection.

- Personal security systems that ensures appropriate approvals or clearance for access official material

- logical access controls that minimize security risks to IT systems

- education and training programs.

Physical Entry Controls:

Protecting organization's physical entry points and protection of secure areas-

1. Authentication controls- card plus personal identification number (PIN)
2. Securely maintained audit trail of access through some form of visible identification worn by all staff
3. Policy based practice of challenging unescorted strangers and anyone not wearing identifications.
4. Regular review and update of access rights to secure areas
5. Appropriate controls for visitors

Controlling Visitors

- Visitors should be
- Issued a pass that is clearly displayed
- Conducted either to the host or a waiting room observed by receptionist or grand.
- Advised that no photography or recording of any type of any time during the visit to areas where classified information is held, processed or handled.
- Asked, where necessary to hand in mobile telephones, cameras, scanners and other recording and communications equipment
- Enrolled in visitors register it should contain name, dept to visit agency or firm, name of employees visited, time of visitor's arrival and departure and reason for the, visit.
- Issued visitors pass.

Entry by media representative

- Designated staff member should accompany media representative throughout visit.
- Classified material should be locked away or at least hidden

- Media representative must be reminded that no photographs or recording of any type may be taken at any time during the visit.

Physical security of facilities rooms and office premises controls for secure zones

- Locate important facilities away from public access
- Lock unattended doors and windows
- Use external protection for windows particularly at ground levels
- Install Intrusion Detection System
  - as per professional standards
  - With regular testing to cover all external doors and accessible windows.
  - To alarm unoccupied areas at all times and others as needed.

-Locate information processing facilities managed by the organization in a different place than those managed by third parties

- Locate support functions and equipment such as photocopies and fax machines in a secure area so that information cannot be compromised.

-Restrict public access to directories and internal access to directories and internal telephone books that the location of sensitive facilities.

- Fireproof safes and security containers for physical protection of Data

-Protecting the premises in which IS are housed from fire hazards

Depends on :

- The security container
- The lock on the container
- The location of the container within the site, building or secure zone.

Physical security through use at cables and locks - Secure work station in with is with anchor pad, a metal pad with lockining rods secured to the surface work station. Many organizations use cables and locks.

Disk locks are another way to secure workstations

The small devices are quickly inserted into diskette slot and lock ant any other diskettes from the unit. They can prevent booting from diskettes and infection from viruses.