Information Security and Network Security

Chapter – 1

Introduction to Information Security

Introduction -

Data is raw Information

Application software

Sources of data – Data entry of data. The real time data collect at source. Data may structure or unstructured.

Date processing cycle

1. Collect Data
2. Store and Organize
3. Processed and transformed data sent to users.

Characteristics of data in sent to transform data quality

1. Reliable source
2. Cannot partial
3. New data doesn't contradict existing data
4. Add value
5. Timely updated

Converting data to information. Presenting data in a way that has meaning and value is called information design.

-Processed form of data is having meaning is called information

-Information in convention that has meaning in some context for its receiver

-Information in derived from data frequently

agricultural Age Industry

Main resources of organization Man, Machine, Money, Material, Management & Information.

Importance data and information

- Improves decision making
- Enhance efficiency
- Provides competitive edge to the organization
- Coordination of business activities in case of distributed and multi-location across the globe.

Why Security of Data and information – feel free from damage. Freedom from threat and feel relax.

Information security – Protects sensitive information from unauthorized activities including insertion, modification, recording and any disruption or destruction. It includes -

- Protection of information systems
- Information processed

Why we use information Security -

- To protect valuable information assets from wide range of threats including theft & cybercrimes.
- To ensure Confidentiality
- Integrity – Accuracy
- Availability Information &Continuity of Service. All Time Available (ATM)

Key reasons why IS

1. Protecting sensitive information
2. Mitigating risk -minimize
3. Compliance with regulations.
4. Protecting reputation.
5. Ensuring business continuity.

Security is Technical Method-

Major concerns

Computer security
Data Security &
Network Security.

Security – Quality or state of being secure.

1. Physical security – Protect physical objects e.g. HDD, RAM etc. from unauthorized users
2. Personal Security- ensures the protection of individual or group of individuals in the organization from Information systems.
3. Operational- to protect the details of a particular project.

Information systems security – Protecting information or data in whatever form of rnedia storage – processing or transit.

Information Security also Called or similar name

- Computer and Network Security
- Information Technology (IT) security
- Information systems Security

- Information and Communication technology (ICT) Security

Basics of Information Systems -

1. Business strategy - Rules and Procedures
2. Software
3. H/W
4. Database
5. Tele Communication or N/W

History of Information Systems –

Information systems (IS) played a crucial role in civilization. It was available in manual forms for Color loading is used to understand.

In mid- 18th century pressures to process data increased. Industry revolution from small shop to factory. Complexity increased. Difficult to manage without the mid of data processing.

In 20th century information – led decision making have increased.

Financial status and future prospects of the business.

Timely and accurate information is essential resource to maintain the operations and to remain competitive.

As with most assets the security of this corporate assets, namely information becomes crucial

Like development in mobile technology or generation of computer systems.

Old days kings send message sealed Information.

- **1960s : Password protection**.
  _ physical measures
  _ No Internet
  _ Prevent access to people
  _ Multiple layers of security protection.
  _ fire safety measures to protect stored data
- **1970s : from CPEEPER to Reaper**
  1971 Frist Computer WORM(Virus) found
  ARPANET – The Advanced Research Project Agency Network.
  Bob Thomas created a computer program CREEPER (Virus) – Program -R replicate itself and spread
  Ray Tomlinson - Wrote program took CREEPER to next level
  Reaper first example of antivirus software.

Thomas and Tomlinson's designed program recovered flaws in APPANET's network security

- **1980s: The Internet**
- Computers more connected
- Viruses become more advanced
- Information security systems could not face innovative hacking approaches.
- 1986 – Russia employed German computer hacker to steal Us military secrets.
- 1988 – network usage began – security measures required become more expensive.
- The worm was designed to propagate across n/w. It gets itself replicated.
- Slow down n/w.
- Computer fraud and missises act.
- CERT-Computer Emergency Response T formed
- WWW launched during 1989.

- **1990s: The rise of Firewalls**
- Internet usage increased
- Data stolen from govt and people via web.
- N/W security Threats had increased exponentially.
- Firewalls and antivirus programs produced.
- NASA researcher created very first firewall program
- Hackers always ahead of Antivirus

- **2000s|:Proper Punishment**
- Govt began clamp down on the Criminals OF HACKING
- Information security Continued to advance as the internet grew
- Hackers quickly become able to create viruses that could not only target specific organization, but whole cities, states and even continents as well.
- NSA- National security Agency.

- **2010s: The era of main breaches (Incidents)**
- Unauthorized Access for Data, applications, N/W or devices.
- Snowden & The NSA 2013 former CI/A (Central Intelligent Agency) employee and contractor for US Government copied and leaked data.
- Yahoo ,2013-2014 Hackers broke into Yahoo; 3 billion user personal information hacked.
- 2017- first 'ransom worm' targeted running MS Windows and demanded payments. In one day, 2,30,000 computers infected across 150 countries.
- Information security is constantly increasing.
- People businesses give top priority to information security
- Implement techniques to ensure that their data stays protected.
- Cloud- based platform to store your personal files

Moving forward

-cyber security becoming stronger

- Cyber Security in a system that responsible for the protection of networks, server and apps that uses the internet.

Goals of Information Security (IS)

IS the collection of practices intended to convey personal information secure from an unapproved/unauthorized access and modification at storing or broadcasting from one place to another place.

Information security is designed and required to secure the print digital and some personal sensitive and private information from unapproved persons.

Major Goals

1. Confidentiality - To prevent unauthorized reading of information. Only sender and predetermined recipient should be able to access information attempt to prevent or unintentional unauthorized disclosure of information. Third party no access.
2. Integrity – When the element of messages is transformed after the sender sends it, but since it reaches the intended recipient, and it can say that principle of the message is lost. Unauthorized writing is prohibited e.g. use of PDF. Some unauthorize user while alter the information while sending data. Modifications are not made by unauthorized personal or process. The data are internally and externally consistent. It should synchronize.
3. Availability - Resources information (Data, H/W, S/W) must be all time available to authorized parties at all times. Ensure the reliable and timely access to data or computing resources of the appropriate personnel. All Time Availability (ATM) of information system i.e. 24x7x365.
4. Message Nonrepudiation -As manual signature on agreement. Message nonrepudiation represent that a sender should not manage to refuse sending message that they send. The burden of data avalanche (sudden arrival of occurrence) on the receiver. Protection against an individual falsely denying having performed a particular action. It is legal concept. Assurance that the sender of information in provided with proof of delivery and the recipient in provided with sender's identity. The inability to deny responsibility for performing a specific act. e.g. Use of digital signature update login details etc.
5. Entity Authentication - The entity or user in authenticated prior to approach to the system resources. e.g. user who in needed to approach the university resources is needed to be authenticated during the login process.
   Physical logical/ software.
6. Access control – The goals of access control determines who should be able to approach what. e.g. who has addition rights should add Deletion/ modification view only rights.

Three pillars of IS

Confidentiality

Integrity Availability

Also, it called CIA triad (enclosed or surrounded).

DAD is reverse of CIA.

D – Disclosure opposite to – confidential.

A – Alteration opposite to integrity

D- Destruction – opposite to availability.

Critical Characteristics of Information

1. Availability –
   - Allows people to access information without being interrupted or obstructed and in the format, they desire.
   - It should available where it in required
2. Accuracy – free from errors or omissions and providing the value that the end -user expects. It is no longer accurate if information has a value that difference from the user's expectations due to purposeful or unintentional content alteration.
3. Authenticity - Reliable – The quality or state of being genuine or original rather than a reproduction or fabrication. Information is authentic when it is the information that was originally created, placed, stored or transferred.
4. Confidentiality (Privacy or secrecy) – The quality or state of perverting disclosure or exposure to unauthorized individuals or systems. Two factor authentication user Id password. Thumb impression etc.
5. Accessible – Accessible management - Information accessible to whom authorize to access. e.g. – some data accessible to top, middle or lower management.

6. Presentable - for top management summary, for middle details for lower actually transaction. Report sequence Higher to Lower, Lower to Higher

7. Relevant - To the word of discussion and decision e.g. for Bonus calculation employee's information for dividend finance information etc.

8. Timely – Important Information required up to seconds e.g. Aeroplan landing. Aircraft / launching space speed /time.

9. Economical –

- Resource cost
- Persons involved
- Space