Information Systems

Chapter 2

Threats of Information System

Protecting Information System Security

-Sanket Mohan Pandhare

Information System Security

- Today most of the IS are connected to internet. Thus they are exposed to the outside world directly.
- Threats from the outside world must be addressed.
- Damage from a non-secure IS can result in catastrophic consequences for the organization.
- Thus organizations must investigate and evaluate the factors that could be a threat.

What Is Information Security?

- Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of the service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

Why Information Security?

- **Cyber crime** is defined as criminal activity involving the IT infrastructure, including illegal access, illegal interception, data interference, misuse of devices, ID theft and electronic fraud.
    - Increased rate of cyber crime issues.
    - Use of IT across businesses
    - Fast growth of Internet
    - Commercialization of Internet
    - Web site defacement
    - Theft of confidential data
    - Financial Frauds
    - Spyware / Adware

Elements of Information Security

Three basic elements of Information Security, which are as follows:

- **Confidentiality**
- **Integrity**
- **Availability**

Confidentiality

- **It is the principle that information will not be disclosed to unauthorized subjects.**

- **Examples:**
  - **Unauthorized network data sniffing**
  - **Listening a phone conversation.**

Integrity

- **It is the protection of system information or process from intentional or accidental unauthorized changes.**

Availability

- **It defines that information or resources are available when required**.

Information Security

- In another words …….

  Information security means making sure to provide required information for the correct people at the correct time.

Other Elements of Information Security

- ***Identification*** – Recognition of an entity by a system.
- ***Authentication*** - Process of verifying identity.
- ***Accountability*** – Tracing activities of individual on a system.
- ***Authorization*** - Granting access or other permissions.
- ***Privacy*** - Right of individual to control the sharing of information about him.

How to achieve Information Security?

- Information Security does not mean only installing antivirus and firewalls.
- Information security tends to protect hardware, software, data, procedures, records, supplies and human resources.
- Information assets are those resources that store, transport, create, use or are information.

How to achieve Information Security?

- **Administrative Controls-** Policies, standards, procedures, guidelines, employee screening, change control, Security awareness trainings.
- **Technical Controls-** Access controls, encryption, Firewalls, IDS, IPS,HTTPS
- **Physical Controls-** Controlled physical access to resources, monitoring, no USB or CDROM etc.

How to achieve Information Security?

Information Security is the responsibility of everyone who can affect the security of a system.

Some Good Habits

- Always use official software.
- Keep all software up-to-date with patches.
- If using free software always download from original developers site.
- Do not disclose all your personal information on social sites like Instagram/Facebook.
- Use Internet with control.
- Use email properly.
- Take care while discarding your E-waste material.
- Use small gadgets carefully as information storage.
- Be careful while surfing from a cybercafe.

Information System Security

- Threat

  A threat is a possible event that can damage or harm an Information System.

- Vulnerability

  It is the weakness within a system. It is the degree of exposure in view of threat.

- Countermeasures

  It is a set of actions implemented to prevent threats.

Information System Security

Network Level Threats

- Attacker requires network access to organization systems or networks.
- Hacking Computers, Implementing Spywares

Information Level Threats

- Attack on the information.
- Sending fake queries to sales department
- Submitting false information.
- Creating revenge web sites.

Information System Security

- Major Security Threats to an IS
  - Computer Crimes / Abuse
  - Human Error
  - Failure of Hardware or Software
  - Natural Disasters
  - Political Disasters

Information System Security

- Computer Crime / Abuse

Computer Viruses

- A code that performs malicious act.
- Can insert itself into other programs in a system.
- Worm is a virus that can replicate itself to other systems using network.
- Biggest threat to personal computing.

Trojan Horse

- A program that performs malicious or unauthorized acts.
- Distributed as a good program.
- May be hidden within a good program.

Information System Security

Denial of Service (DoS)

- Making system unavailable to legitimate users.

Impersonation

- Assuming someone else's identity and enjoying his privileges.

Salami Technique

- Diverting small amount of money from a large number of accounts maintained by the system.
- Small amounts go unnoticed.

Spoofing

- Configuring a computer to assume some other computers identity.

Information System Security

Data Leakage

- Various techniques are used to obtain stored data
  - SQL injection
  - Error Outputs

Wiretapping

- Tapping computer transmission lines to obtain data.

Theft of Mobile Devices

Information System Security

Myths, rumors and hoaxes

- Created by sending false emails to as many people as possible.
- These may have significant impact on companies, their reputation and business.

Web Site Attacks

- Web site defacement
- Adding wrong information

Increase in cyber crime rates

- Organized cyber criminals

Information System Security

Employee Issues

- Disgruntle Employees
- Availability of hacking tools

Social Engineering Attacks

- Sharing Passwords
- Sharing Official Systems

Rise in Mobile workers

- Use mobile devices
- Wireless access

Classification of Threats

- Four things to be considered while evaluating threat

- Asset

Something of value to the organization

- Actor / Attacker

Who or what may violate the security requirement

- Motive

Deliberate or accidental

- Access

How the attacker will access the asset.

Classification of Threats

- Types of assets

Hardware
Software
Information
Systems
People

Classification of Threats

Classify Assets

- Tag Assets based on their value to the organization.
- Find various threats to important assets.
- Tag threats for an asset.
- Find the threats which have maximum risk.
- Calculate the loss due to these threats.

Cost of Threats

- Cost of a threat can be calculated considering following factors
  - Productivity
    - No. of employees affected
    - No. of hours wasted
    - Cost per hour / per employee
  - Revenue
    - Direct financial loss
    - Future business loss
    - Financial Performance
    - Credit rating and stock price
  - Hidden Costs

Information System Security

- The aim of the information system security is to protect organization assets.
- If not fully protected at least limit damage to them.
- Limit access to information to authorized users only.
- Information systems controls play a crucial role to ensure secure operations of IS.
- They safeguard the assets and the data within them.

Information System Security

- The organization needs to develop a set of security policies, procedures and technological measures.
- Information System Controls-
  - Preventive Controls
    - Prevent an error or attack
  - Detective Controls
    - Detect a security breach or incident
  - Corrective Controls
    - These control detect any error or incident and correct it.

Summary

- **Information security means making sure to provide required information for the correct people at the correct time.**
- CIA Traid
- Computer Crime/Abuse: Worms, Trojans, Adware's, etc.
- Classification of Threats