Introduction to Information Security

What is information?

- Information is associated with data.
- Information is like an asset to an individual/ organization that needs to be protected.
- Information is expressed either as the content of a message or through direct or indirect observation.
- Information can be encoded into various forms for transmission and interpretation.
- It can also be encrypted for safe storage and communication.

Information

- Created, destroyed, used, stored, processed, transferred, lost, stolen
- Printed on a paper and locked in a file cabinet.
- Recorded electronically and available on the network.
- Spoken verbally.
- Transferred by post or electronically.

What is Information Security?

- Practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.
- Application of measures to ensure safety and privacy of data by managing its storage and distribution.
- Spans so many research areas like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media etc.
- Necessary tools: policy, education, awareness, training, technology

Need of Information Security

- To make sure business continuity and scale back business injury by preventing and minimizing the impact of security incidents.
- Protecting the functionality of the organization
  - organizations must set policy
- Enabling the safe operation of applications
  - safeguards important application using the organization's IT systems
- Protecting the data that the organization collect and use
  - protection of both data in motion as well as data in rest
- Safeguarding technology assets in organizations
  - need for public key infrastructure, PKI an integrated system of the software, encryption methodologies

Examples

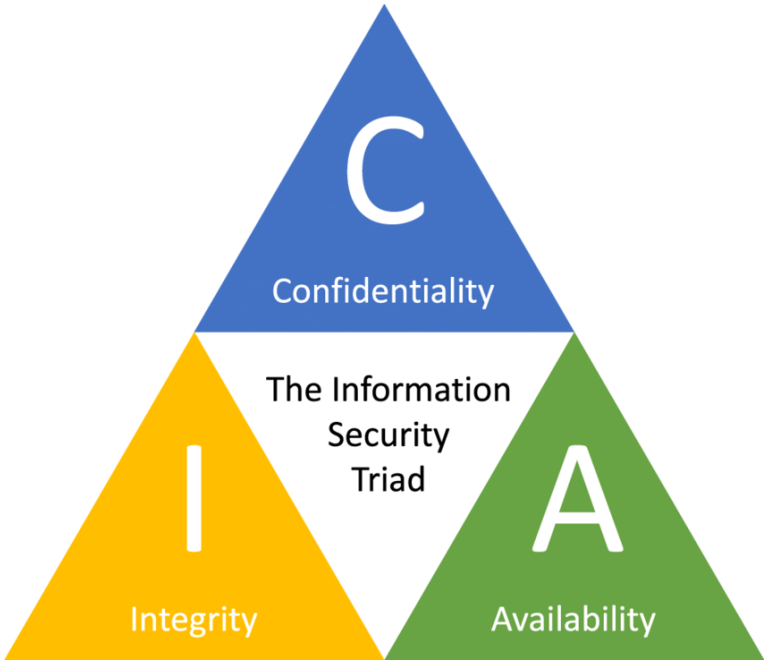
- Not patching our systems
- Using weak passwords such as “password” or “1234”
- Downloading programs from the Internet
- Opening e-mail attachments from unknown senders
- Using wireless networks without encryption

Information Security vs. Cyber Security

- *Value of Data*: CS tries to safeguard your organization's commercial information and protect IT systems from digital hacking activities that could result in valuable data being accessed. IS is aimed at protecting the value of your company's information assets from any type of threat, digital or not.
- *Security professional priorities*: CS professionals are most concerned with preventing active threats, such as hacking attempts and viruses. On the other hand, IS professionals have a broader remit, including policies, procedures, and organizational roles and responsibilities to ensure confidentiality, integrity, and availability.
- *Focus of infosec vs cybersec*: CS focuses on establishing protection from digital threats arising outside the organization. IS focuses on implementing policies and procedures to protect the confidentiality, integrity, and availability of all types of information asset.
- *Threats:* CS is only concerned with cyber threats. IS is concerned with threats of all types.

Basic Security Concepts

- The CIA triad
  - Confidentiality: controlling who gets to read information;
  - Integrity: assuring that information and programs are changed only in a specified and authorized manner
  - Availability: assuring that authorized users have continued access to information and resources.



Security breach leads to..

- Loss of confidentiality
  - Interception
- Loss of integrity
  - Interruption
  - Modification
  - Fabrication
- Loss of availability
  - Interruption
  - Modification
  - Fabrication
- Denial of service

Responding to breaches..

- Authorization
  - a particular user (or computer system) has the right to carry out a certain activity
  - reading a file or running a program
- Authentication
  - proving that a user is the person he or she claims to be.
  - involve something the user knows (such as a password), something the user has (such as a “smartcard”), or something about the user that proves the person’s identity (such as a fingerprint).
- Non-repudiation
  - Security is strong when the means of authentication cannot later be refuted
  - the user cannot later deny that he or she performed the activity

Threat, Risk, Vulnerabilities

- T: Something that has the potential to cause us harm.
- V: Weaknesses that can be exploited by threats in order to cause us harm.
- R: Likelihood that something bad will happen. A threat and a vulnerability that the specific threat can exploit.
- I: Value of the asset being threatened to be a factor

Threat: Something that can damage or destroy an asset

Vulnerability: A weakness or gap in your protection

Risk: Where assets, threats, and vulnerabilities intersect

Security Threats

- Intrusion – Unauthorized individuals trying to gain access to computer systems in order to steal information
- Virus, Worm, Trojan Horse (Malware) – Programs that infect your machine and carry malicious codes to destroy the data on your machine or allow an intruder to take control over your machine
- Phishing – The practice of using email or fake website to lure the recipient in providing personal information
- Spyware – Software that sends information from your computer to a third party without your consent
- Spam – Programs designed to send a message to multiple users, mailing lists or email groups

Security Risks

- Compromised Personally Identifiable Information (PII); PII data refers to name, SSN, Licenses, bank accounts
- Identity Theft- computer intruders intent on stealing your personal information to commit fraud or theft
- The use of non-secure settings of peer-to-peer File Sharing applications.
- Compromised computer; A computer experiencing unexpected and unexplainable
  - Disk activities
  - Performance degradation
  - Repeated login failure or connections to unfamiliar services

Or a stolen or lost computer

Impact on work?

Questions:

- How would you know whether an email sent to you with an attachment is free from viruses?
- How do you secure sensitive data you send via email?
- What steps would you take to secure your computer from malware?
- What does the phrase “safely manage your password” mean to you?

Security Measures

- Safely mange your password
- Safely manage your email account
- Secure your computer
- Protect the data you are handling
- Avoid risky behavior online
- Be aware of security guidelines, policies, and procedures

Security policies

Identification and Authentication

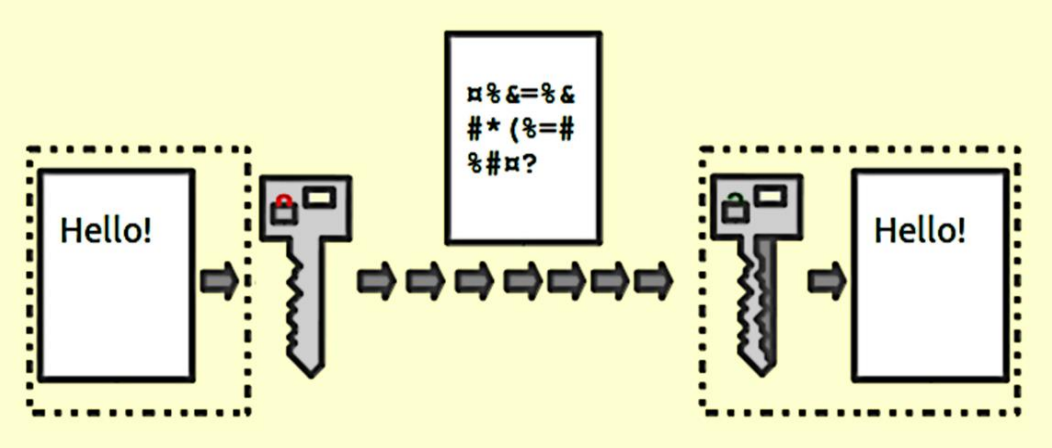
- Persons accessing the information is who they say they are
- Factors of identification:
  - Something you know – user ID and password
    - User ID identifies you while the password authenticates you
    - Easy to compromise if weak password
  - Something you have – key or card
    - Can be lost or stolen
  - Something you are – physical characteristics (i.e., biometrics)
    - Much harder to compromise
- A combination of at least 2 factors is recommended

Access Control

- Once authenticated – only provide access to information necessary to perform their job duties to read, modify, add, and/or delete information by:
  - Access control list (ACL) created for each resource (information)
    - List of users that can read, write, delete or add information
    - Difficult to maintain all the lists
  - Role-based access control (RBAC)
    - Rather than individual lists
    - Users are assigned to roles
    - Roles define what they can access
    - Simplifies administration

Encryption

- An algorithm (program) encodes or scrambles information during transmission or storage
- Decoded/unscrambled by only authorized individuals to read it



- How is this done?
  - Both parties agree on the encryption method (there are many) using keys
    - Symmetric key – sender and receiver have the key which can be risky
    - Public Key – use a public and private key where the public key is used to send an encrypted message and a private key that the receiver uses to decode the message

Backup

- Important information should be backed up and store in a separate location:
  - Very useful in the event that the primary computer systems become unavailable
- A good backup plan requires:
  - Understanding of the organizational information resources
  - Regular backups of all data
  - Offsite storage of backups
  - Test of the data restoration
- Complementary practices:
  - UPS systems
  - Backup processing sites

Physical Security

- Protection of the actual equipment
  - Hardware
  - Networking components
- Organizations need to identify assets that need to be physically secured:
  - Locked doors
  - Physical intrusion detection - e.g., using security cameras
  - Secured equipment
  - Environmental monitoring – temperature, humidity, and airflow for computer equipment
  - Employee training

Firewalls

- Can be a piece of hardware and/or software
- Inspects and stops packets of information that don't apply to a strict set of rules
  - Inbound and outbound
- Hardware firewalls are connected to the network
- Software firewalls run on the operating system and intercepts packets as they arrive to a computer
- Can implement multiple firewalls to allow segments of the network to be partially secured to conduct business
- Intrusion Detection Systems (IDS) watch for specific types of activities to alert security personnel of potential network attack