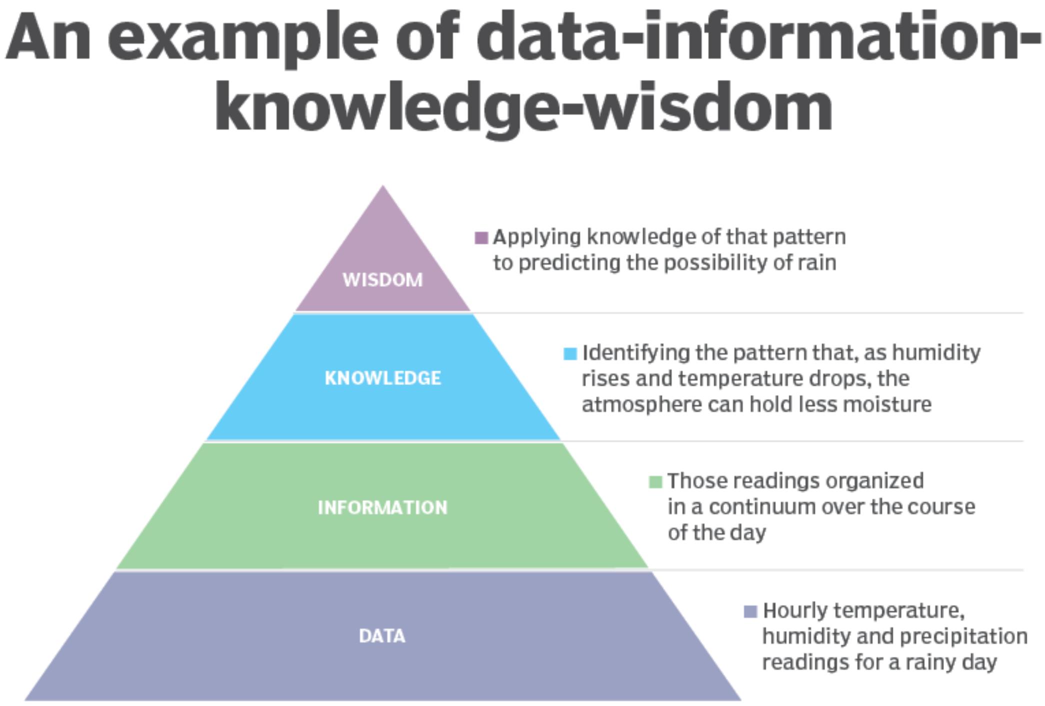
Introduction to Information System Security (Chapter 1, BCIS)

Information:

Information is the organized and processed form of data. In general, data refers to the numerical and quantitative entity. When this irregular quantitative data is organized, structured and processed it becomes information. For eg. data of daily rainfall can be grouped, organized and analysed further to understand that it rains more in summer as compared to winter, also, it rains more in the Terai region as compared to Hilly regions.


An example of data-information-knowledge-wisdom

Applying knowledge of that pattern to predicting the possibility of rain

Identifying the pattern that, as humidity rises and temperature drops, the atmosphere can hold less moisture

Those readings organized in a continuum over the course of the day

Hourly temperature, humidity and precipitation readings for a rainy day

Information System

Information system, an integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products. Business firms and other organizations rely on information systems to carry out and manage their operations, interact with their customers and suppliers, and compete in the marketplace. Information systems are used to run interorganizational supply chains and electronic markets. For instance, corporations use information systems to process financial accounts, to manage their human resources, and to reach their potential customers with online promotions. Many major companies are built entirely around information systems. These include eBay, a largely auction marketplace; Amazon, an expanding electronic mall and provider of cloud computing services; Alibaba, a business-to-business e-marketplace; and Google, a search engine company that derives most of its revenue from keyword advertising on Internet searches. Governments deploy information systems to provide services cost-effectively to citizens. Digital goods—such as electronic books, video products, and software—and online services, such as gaming and social networking, are delivered with information systems. Individuals rely on information systems, generally Internet-based, for conducting much of their personal lives: for socializing, study, shopping, banking, and entertainment.

Security

The state of being free from threat or danger. Security is protection. Protection from adversaries—those who would do harm, intentionally or otherwise—is the ultimate objective of security. A successful organization should have multiple layers of security in place to protect its operations, physical infrastructure, people, functions, communications, and information.

For eg. we feel secure inside our home when doors are locked.

Information Security

- methods, tools and personnel used to defend an organization's or individual digital assets.
- The goal of IT security is to protect these assets, devices and services from being disrupted, stolen or exploited by unauthorized users, otherwise known as threat actors.
- protection of information and its critical elements, including the systems and hardware that use, store, and transmit the information.
- It includes the broad areas of information security management, data security, and network security.
- An effective security strategy uses a range of approaches to minimize vulnerabilities and target many types of cyberthreats.
- Detection, prevention and response to security threats involve the use of security policies, software tools and IT services.
- Unfortunately, technological innovation benefits both IT defenders and cybercriminals.
- To protect business assets, companies must routinely review, update and improve security to stay ahead of cyberthreats and increasingly sophisticated cybercriminals.

Physical Security of Information systems is vital when it comes to Information security. Protection of people, hardware, software, network information and data from physical actions, intrusions and other events that could damage an organization and its assets. Protecting it from threat actors, as well as accidents and natural disasters, such as fires, floods, earthquakes and severe weather.

There are three parts to physical security:

- access control
    - Controlling access to office buildings, research centers, laboratories, data centers and other locations is vital to physical security
    - Biometric recognition
- Surveillance
    - technologies and tactics used to monitor activity in and around facilities and equipment.
    - Cameras
    - Thermal Sensors
    - Motion Detectors
    - Security Alarms
- Testing
    - Penetration Testing

Key Information Security Concepts

- Access: A subject or object's ability to use, manipulate, modify, or affect another subject or object.hackers must gain illegal access to a system.
- Asset: The organizational resource that is being protected.
    - Logical asset:Website, software information, or data;
    - Physical asset: such as a person, computer system, hardware, or other tangible object.

- Attack: An intentional or unintentional act that can damage or otherwise compromise information and the systems that support it. Attacks can be active or passive, intentional or unintentional, and direct or indirect.
    - Active: attacker tries to modify the content
    - Passive: attacker reads the information for long period of time
    - Intentional: Hacker using a pc ant conducting attack
    - Unintentional: Earthquake disrupting the operation
    - Direct: Attack directly from hacker
    - Indirect: Attack from compromised system initiated by a hacker

- Control, safeguard, or countermeasure: Security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve security within an organization. The various levels and types of controls are discussed more fully in the following chapters.
- Exploit (शोषण):

    - technique used to compromise a system.
    - to take advantage of a vulnerability or exposure, usually in software
- Exposure: the revelation of something secret, especially something damaging.
- Protection profile or security posture: Entire set of controls and safeguards, including policy, education, training and awareness, and technology, that the organization implements to protect the asset.
- Vulnerability – Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset.
- Threat – Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.
- Risk: The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.
- Subject and Object: Subject- device used to attack a system, Object: device being attacked
- Threat agent/actor: party that is responsible for, or attempts to bring about, harm to an organization. “Particular hacker”
- Threat event: An occurrence of an event caused by a threat agent. “Data breach event”
- Threat source: A category of objects, people, or other entities that represents the origin of danger to an asset—in other words, a category of threat agents. “Hackers”

The History of Information Security

This section will be covered separately.

Components of an Information System

Information system (IS) The entire set of software, hardware, data, people, procedures, and networks that enable the use of information resources in the organization.

Security of an Information System is possible only when all of its individual components are protected.

Software

The software component of an IS includes applications (programs), operating systems, and assorted command utilities. It is one of the most difficult to protect and the most vulnerable component of the Information System.

Hardware

Hardware is the physical technology that houses and executes the software, stores and transports the data, and provides interfaces for the entry and removal of information from the system. Physical security policies deal with hardware as a physical asset and with the protection of physical assets from harm or theft.

Data

Data stored, processed, and transmitted by a computer system must be protected. Data is often the most valuable asset of an organization and therefore is the main target of intentional attacks.

People

Employees safeguarding the IS or people taking services from IS are also a great threat to the IS. The most convenient and promising way of compromising IS is through social engineering in which the role of people is the must.

Procedures

Procedures is the set of written directives/instructions to perform a task. Each and every action related to operation and maintenance of IS must adhere with predetermined procedures. But it’s knowledge must be disseminated among many employees rather than just an employee to keep the data safer.

Network

Connection of two or more computers is known as a network. Networking gives us a large scale ability in the computing domain. It is a pathway for data hence it must be much more secure than the data storing and processing facility. Installing and configuring firewalls, implementing intrusion prevention systems (IPS) can help keep the network safe.

Critical Characteristics of Information (Expanded CIA Triad)

The value of information comes from the character it possesses. Depending upon its characteristics it might be valuable, meaningful or not at all.

Availability:

Availability enables authorized users—people or computer systems—to access information without interference or obstruction and to receive it in the required format and necessary time.

Accuracy:

Information has accuracy when it is free from mistakes or errors and has the value that the end user expects.

Authenticity:

Authenticity is the quality or state of being genuine, original rather than reproduction or fabrication. It must not change during storage or transmission to maintain authenticity.

Confidentiality:

Information has confidentiality when it is protected from disclosure or exposure to unauthorized individuals or systems but is accessible to rightful, privileged users. Confidentiality is closely related to privacy.

Integrity:

Information has integrity when it is whole, complete, and uncorrupted. The integrity of information is threatened when it is exposed to corruption, damage, destruction of its authentic state. Corruption can occur while information is being stored or transmitted. Many computer viruses and worms are designed with the explicit purpose of corrupting data.

Utility:

Utility of information is the state of having value for some purpose to the end users. OR, info. has utility when it has some value.

Possession:

The possession of information is the quality or state of ownership or control. While a breach of confidentiality always results in a breach of possession, a breach of possession does not always lead to a breach of confidentiality.

Balancing Information Security and Access

It is almost impossible to obtain an absolutely secure IS. More vulnerabilities will be exposed in the near future for the system considered to be extremely robust at present. Considering every circumstance IS must be able to provide the access to the authorized person at the same time restricting the unauthorized users. Information can be made available to anyone, anywhere, anytime by any medium. But such kind unrestricted access poses a great danger. On the other hand, a very strict security policy might not allow the authorised users when they need to.

To achieve balance- IS must satisfy the users as well as the security professionals. The security policy must allow the authorised users to the need based resources, whereas, recognize and restrict the unauthorised users to access the sensitive IS. Hence, this critical balance must allow authorised users to access the necessary resources wherever and whenever they need with minimum delay and obstacles.

Need for Information Security

- **Protecting the organization’s ability to function**
    - The three communities of interest—general management, IT management, and information security management—are each responsible for facilitating the information security program that protects the organization’s ability to function. Each of an organization’s communities of interest must address information security in terms of business impact and the cost of business interruption, rather than isolating security as a technical problem.
- **Protecting the data and information the organization collects and uses, whether physical or electronic**
    - Any business, government agency, educational institution which relies on an information system loses its record of transactions and its ability to deliver value to customers when it loses data.
    - protecting data in transmission, in processing, and at rest (storage).
    - The value of data motivates attackers to steal, sabotage, or corrupt it.
    - Protection of dbms.
    - Managerial controls include policy, procedure, and governance.
    - Technical controls rely on knowledge of access control, authentication, auditing, application security, backup and recovery, encryption, and integrity controls.
    - Physical controls include the use of data centers with locking doors, fire suppression systems, video monitoring, and physical security guards.
- **Enabling the safe operation of applications running on the organization’s IT systems**
    - Every organization depends on many applications.
    - operating system platforms, certain operational applications, electronic mail (e-mail), and instant messaging (IM) applications, like text messaging (short message service, or SMS).
    - They either build their own or purchase from external parties. Once these elements are in place, management must responsively oversee it instead of relegating it’s management to the IT department.
- **Safeguarding the organization’s technology assets**
    - According to the size and need of an organization every organization owns or uses various kinds of hardware, software and solutions.
    - With time these requirements change.

- Startup uses a small router, small-scale firewall or none. Once it grows to medium scale it might require a firewall with IDS and IPS.
- Safeguarding these tech assets is vital.

References:

1. Principles of Information Security by Michael E. Whitman & Herbert J. Mattord
2. Britannica.com
3. Techtarget.com
4. Computerweekly.com