LESSON 10: INFORMATION SYSTEM SECURITY

The term security is easiest to define by breaking it into pieces. An **information system** consists of the hardware, operating system, and application software that work together to collect, process, and store data for individuals and organizations.

Security as a condition is the degree of resistance to, or protection from, harm. It applies to any vulnerable and valuable asset, such as a person, dwelling, community, nation, or organization. Establishing or maintaining a sufficient degree of security is the aim of the work, structures, and processes called "security."

Thus **information systems security** is the collection of activities that protect the information system and the data stored in it. **Information security** means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Adversaries of information system security

To understand how to make computers more secure, you first need to understand the concepts of risks, threats, and vulnerabilities.

- **Risk** is the likelihood that something bad will happen to an asset. It is the level of exposure to some event that has an effect on an asset. In the context of IT security, an asset can be a computer, a database, or a piece of information. Examples of risk include the following:
    - Losing data
    - Losing business because a disaster has destroyed your building
    - Failing to comply with laws and regulations

It has two components:

Risk Exposure = Probability * Damage Potential (Consequence/loss)

This formula indicates that the risk posed by a particular threat is equal to the probability of the threat occurring multiplied by the damage potential, which indicates the consequences to your system if an attack were to occur.

- **A threat** is any action that could damage an asset. Information systems face both natural and human-induced threats. The threats of flood, earthquake, or severe storms require organizations to create plans to ensure that business operation continues and that the organization can recover. A business continuity plan (BCP) gives priorities to the functions an organization needs to keep going. A disaster recovery plan (DRP) defines how a business gets back on its feet after a major disaster such as a fire or hurricane. Human-caused threats to a computer system include viruses, malicious code, and unauthorized access. A virus is a computer program written to cause damage to a system, an application, or data. Malicious code, or malware, is a computer program written to cause a specific action to occur, such as erasing a hard drive. These threats can harm an individual, business, or organization.

- **A vulnerability** is a weakness that allows a threat to be realized or to have an effect on an asset. To understand what a vulnerability is, think about lighting a fire. Lighting a fire is not necessarily bad. If you are cooking a meal on a grill, you will need to light a fire in the grill. The grill is designed to contain the fire and should pose no danger if used properly. On the other hand, lighting a fire in a computer data center will likely cause damage. A grill is not vulnerable to fire, but a computer data center is. A threat by itself does not always cause damage; there must be a vulnerability for a threat to be realized.

CORE PRINCIPLES OF INFORMATION SECURITY

i. Confidentiality

Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information.

Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds.

ii. Integrity

In information security, integrity means that data cannot be modified undetectably. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of Consistency as understood in the classic ACID model of transaction processing. Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

iii. Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

iv. Authenticity

In computing, e-Business and information security it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are.

v. Non-repudiation

In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation.

CONTROLS

When Management chooses to mitigate a risk, they will do so by implementing one or more of three different types of controls.

i. Administrative Controls

Administrative controls (also called procedural controls) consist of approved written policies, procedures, standards and guidelines. Administrative controls form the framework for running the business and managing people. They inform people on how the business is to be run and how day to day operations are to be conducted. Laws and regulations created by government bodies are also a type of administrative control because they inform the business. Some industry sectors have policies, procedures, standards and guidelines that must be followed - the Payment Card Industry (PCI) Data Security Standard required by Visa and Master Card is such an example. Other examples of administrative controls include the corporate security policy, password policy, hiring policies, and disciplinary policies.

Administrative controls form the basis for the selection and implementation of logical and physical controls. Logical and physical controls are manifestations of administrative controls. Administrative controls are of paramount importance.

ii. Logical controls

Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems. For example: passwords, network and host based firewalls, network intrusion detection systems, access control lists, and data encryption are logical controls.

An important logical control that is frequently overlooked is the principle of least privilege. The principle of least privilege requires that an individual, program or system process is not granted any more access privileges than are necessary to perform the task. A blatant example of the failure to adhere to the principle of least privilege is logging into Windows as user Administrator to read Email and surf the Web. Violations of this principle can also occur when an individual collects additional access privileges over time. This happens when employees' job duties change, or they are promoted to a new position, or they transfer to another department. The access privileges required by their new duties are frequently added onto their already existing access privileges which may no longer be necessary or appropriate.

iii. Physical Control

Physical controls monitor and control the environment of the work place and computing facilities. They also monitor and control access to and from such facilities. For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the network and work place into functional areas are also physical controls.

An important physical control that is frequently overlooked is the separation of duties. Separation of duties ensures that an individual cannot complete a critical task by himself. For example: an employee who submits a request for reimbursement should not also be able to authorize payment or print the check. An applications programmer should not also be the server administrator or the database administrator - these roles and responsibilities must be separated from one another.