**Class Note 2**

**What is Security?**

**Security** is “the quality or state of being secure—to be free from danger.” In other words, protection against adversaries—from those who would do harm, intentionally or otherwise.

A successful organization should have the following multiple layers of security in place to protect its operations:

* **Physical security**, to protect physical items, objects, or areas from unauthorized access and misuse
* **Personnel security**, to protect the individual or group of individuals who are authorized to access the organization and its operations
* **Operations security**, to protect the details of a particular operation or series of activities
* **Communications security**, to protect communications media, technology, and content
* **Network security**, to protect networking components, connections, and contents
* **Information security**, to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology.

The Committee on National Security Systems (CNSS) defines information security as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.

Information security includes the broad areas of information security management, computer and data security, and network security. The CNSS model of information security evolved from a concept developed by the computer security industry called the C.I.A. triangle. The **C.I.A. triangle** has been the industry standard for computer security since the development of the mainframe. It is based on the three characteristics of information that give it value to organizations: confidentiality, integrity, and availability.

Note: the C.I.A. triangle model no longer adequately addresses the constantly changing environment. The threats to the confidentiality, integrity, and availability of information have evolved into a vast collection of events, including accidental or intentional damage, destruction, theft, unintended or unauthorized modification, or other misuse from human or nonhuman threats. Thus, development of a more robust model that addresses the complexities of the current information security environment is required.

**Key Information Security Concepts**

**Access:** A subject or object’s ability to use, manipulate, modify, or affect another subject or object. Authorized users have legal access to a system, whereas hackers have illegal access to a system. Access controls regulate this ability.

**Asset:** The organizational resource that is being protected. An asset can be logical, such as a Web site, information, or data; or an asset can be physical, such as a person, computer system, or other tangible object. Assets, and particularly information assets, are the focus of security efforts; they are what those efforts are attempting to protect.

**Attack:** An intentional or unintentional act that can cause damage to or otherwise compromise information and/or the systems that support it. Attacks can be active or passive, intentional or unintentional, and direct or indirect.

* Someone casually reading sensitive information not intended for his or her use is a passive attack.
* A hacker attempting to break into an information system is an intentional attack.
* A lightning strike that causes a fire in a building is an unintentional attack.
* A direct attack is a hacker using a personal computer to break into a system.
* An indirect attack is a hacker compromising a system and using it to attack other systems (i.e. case of a botnet).

Direct attacks originate from the threat itself. Indirect attacks originate from a compromised system or resource that is malfunctioning or working under the control of a threat.

**Control, safeguard,** or **countermeasure:** Security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve the security within an organization.

**Exploit** (n/v)**:** A technique used to compromise a system. Threat agents may attempt to exploit a system or other information asset by using it illegally for their personal gain. Or, an exploit can be a documented process to take advantage of a vulnerability or exposure, usually in software, that is either inherent in the software or is created by the attacker. Exploits make use of existing software tools or custom-made software components.

**Exposure:** A condition or state of being exposed. In information security, exposure exists when a vulnerability known to an attacker is present.

**Loss:** A single instance of an information asset suffering damage or unintended or unauthorized modification or disclosure. When an organization’s information is stolen, it has suffered a loss.

**Protection profile** or **security posture:** The entire set of controls and safeguards, including policy, education, training and awareness, and technology, that the organization implements (or fails to implement) to protect the asset.

**Risk:** The probability that something unwanted will happen. Organizations must minimize risk to match their **risk appetite**—the quantity and nature of risk the organization is willing to accept.

**Subjects** and **objects:** A computer can be either the **subject** of an attack—an agent entity used to conduct the attack—or the **object** of an attack—the target entity. A computer can be both the subject and object of an attack, when, for example, it is compromised by an attack (object), and is then used to attack other systems (subject).

**Threat:** A category of objects, persons, or other entities that presents a danger to an asset. Threats are always present and can be purposeful or undirected. For example, hackers purposefully threaten unprotected information systems, while severe storms incidentally threaten buildings and their contents.

**Threat agent:** The specific instance or a component of a threat. For example, all hackers in the world present a collective threat, while Kevin Mitnick, who was convicted for hacking into phone systems, is a specific threat agent. Likewise, a lightning strike, hailstorm, or tornado is a threat agent that is part of the threat of severe storms.

**Vulnerability:** A weaknesses or fault in a system or protection mechanism that opens it to attack or damage. Some examples of vulnerabilities are a flaw in a software package, an unprotected system port, and an unlocked door.

**Critical Characteristics of Information**

The value of information comes from the characteristics it possesses. When a characteristic of information changes, the value of that information either increases, or, more commonly, decreases. Some characteristics affect information’s value to users more than others do. This can depend on circumstances; for example, timeliness of information can be a critical factor, because information loses much or all of its value when it is delivered too late.

Each critical characteristic of information—i.e., the expanded C.I.A. triangle—is defined as follows:

**Availability:** enables authorized users—persons or computer systems—to access information without interference or obstruction and to receive it in the required format.

**Accuracy:** Information has **accuracy** when it is free from mistakes or errors and it has the value that the end user expects. If information has been intentionally or unintentionally modified, it is no longer accurate.

**Authenticity: Authenticity** of information is the quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is in the same state in which it was created, placed, stored, or transferred.

* **E-mail spoofing** - the act of sending an e-mail message with a modified field. Spoofing the sender’s address can fool e-mail recipients into thinking that messages are legitimate traffic, thus inducing them to open e-mail they otherwise might not have.
* **phishing**, when an attacker attempts to obtain personal or financial information using fraudulent means, most often by posing as another individual or organization. When used in a phishing attack, e-mail spoofing lures victims to a Web server that does not represent the organization it purports to, in an attempt to steal their private data such as account numbers and passwords.

Difference: Spoofing downloads malware to your computer, or network while phishing tricks you into giving up sensitive financial information to a cyber-crook.

**Confidentiality:** Information has **confidentiality** when it is protected from disclosure or exposure to unauthorized individuals or systems. Confidentiality ensures that *only* those with the rights and privileges to access information are able to do so. When unauthorized individuals or systems can view information, confidentiality is breached.

Some of the measures used to protect the confidentiality of information are:

* Information classification
* Secure document storage
* Application of general security policies
* Education of information custodians and end users

\* Confidentiality is interdependent with other characteristics and is most closely related to the privacy. Examples: unintentional disclosures, an employee throwing away a document containing critical information without shredding it, or a hacker who successfully breaks into an internal database of a Web-based organization and steals sensitive information about the clients, such as names, addresses, and credit card numbers.

\* In information security, **salami theft** occurs when an employee steals a few pieces of information at a time, knowing that taking more would be noticed—but eventually the employee gets something complete or useable.

**Integrity** Information has **integrity** when it is whole, complete, and uncorrupted. The integrity of information is threatened when the information is exposed to corruption, damage, destruction, or other disruption of its authentic state.

\* Information integrity is the cornerstone of information systems, because information is of no value or use if users cannot verify its integrity.

**Utility: the** **utility** of information is the quality or state of having value for some purpose or end. Information has value when it can serve a purpose. If information is available, but is not in a format meaningful to the end user, it is not useful.

**Possession:** The **possession** of information is the quality or state of ownership or control. Information is said to be in one’s possession if one obtains it, independent of format or other characteristics. While a breach of confidentiality always results in a breach of possession, a breach of possession does not always result in a breach of confidentiality.

**Components of an Information System**

**Information System (IS)** is the entire set of software, hardware, data, people, procedures, and networks that make possible the use of information resources in the organization.

1. **Software -** The software component of the IS comprises applications, operating systems, and assorted command utilities. Software is perhaps the most difficult IS component to secure. The exploitation of errors in software programming accounts for a substantial portion of the attacks on information. Software carries the lifeblood of information through an organization.

2. **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.

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

4. **People** – People can be the weakest link in an organization’s information security program. And unless policy, education and training, awareness, and technology are properly employed to prevent people from accidentally or intentionally damaging or losing information, they will remain the weakest link. Social engineering can prey on the tendency to cut corners and the commonplace nature of human error. It can be used to manipulate the actions of people to obtain access information about a system.

5. **Procedures** - Procedures are written instructions for accomplishing a specific task. When an unauthorized user obtains an organization’s procedures, this poses a threat to the integrity of the information.

6. **Networks** - component that created much of the need for increased computer and information security. When information systems are connected to each other to form local area networks (LANs), and these LANs are connected to other networks such as the Internet, new security challenges rapidly emerge.

**Security Professionals and the Organization**

Senior Management: The senior technology officer is typically the **chief information officer (CIO).** The CIO is primarily responsible for advising the chief executive officer, president, or company owner on the strategic planning that affects the management of information in the organization. The CIO translates the strategic plans of the organization as a whole into strategic information plans for the information systems or data processing division of the organization. Once this is accomplished, CIOs work with subordinate managers to develop tactical and operational plans for the division and to enable planning and management of the systems that support the organization.

The **chief information security officer (CISO)** has primary responsibility for the assessment, management, and implementation of information security in the organization. The CISO may also be referred to as the manager for IT security, the security administrator, or a similar title.

**Information Security Project Team**

The information security **project team** should consist of a number of individuals who are experienced in one or multiple facets of the required technical and nontechnical areas.

Members of the security project team fill the following roles:

**Champion:** A senior executive who promotes the project and ensures its support, both financially and administratively, at the highest levels of the organization.

**Team leader:** A project manager, who may be a departmental line manager or staff unit manager, who understands project management, personnel management, and information security technical requirements.

**Security policy developers:** People who understand the organizational culture, existing policies, and requirements for developing and implementing successful policies.

**Risk assessment specialists:** People who understand financial risk assessment techniques, the value of organizational assets, and the security methods to be used.

**Security professionals:** Dedicated, trained, and well-educated specialists in all aspects of information security from both a technical and nontechnical standpoint.

**Systems administrators:** People with the primary responsibility for administering the systems that house the information used by the organization.

**End users:** Those whom the new system will most directly affect. Ideally, a selection of users from various departments, levels, and degrees of technical knowledge assist the team in focusing on the application of realistic controls applied in ways that do not disrupt the essential business activities they seek to safeguard.

References

[1] Principle of Information Security by Michael E. Whitman, 5th Edition, Herbert J. Mattord.

[2] Network Security Essentials: Applications and Standards, 4th Edition, William Stallings.