# **Chapter 1**

**Introduction to Information Security**

|  |
| --- |
| **At a Glance** |

#### Instructor’s Manual Table of Contents

* Overview
* Objectives
* Teaching Tips
* Quick Quizzes
* Class Discussion Topics
* Additional Projects
* Additional Resources
* Key Terms

|  |
| --- |
| Lecture Notes |

# **Overview**

Network security is a critical component in the day-to-day IT operations of nearly every organization in business today. This chapter offers an overview of the entire field of information security and its effects on network security.

# **Objectives**

* Explain the relationships among the component parts of information security, especially network security
* Define the key terms and critical concepts of information and network security
* Explain the business need for information and network security
* Identify the threats posed to information and network security, as well as the common attacks associated with those threats
* Distinguish between threats to information from within systems and attacks against information from within systems
* Describe the organizational roles of information and network security professionals
* Define management’s role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines
* Discuss how an organization institutionalizes policies, standards, and practices using education, training, and awareness programs

# **Teaching Tips**

**Introduction**

1. Before learning how to plan, design, and implement network security, it is important that students understand the larger topic of information security and how the components of network security fit into this topic.

**What Is Information Security?**

1. Information security (InfoSec) is the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information. Note that in order to protect information and its related systems, organizations must integrate the following security layers:

* Network security
* Physical security
* Personal security
* Operations security
* Communications security

**Information Security Terminology**

1. The following terms and concepts are essential to any discussion of information security (use Figures 1-1 and 1-2 to aid the discussion):

* Access
* Asset
* Attack
* Control, safeguard, or countermeasure
* Exploit
* Exposure
* Intellectual Property
* Loss
* Protection profile or security posture
* Risk
* Subjects
* Threat
* Threat agent
* Vulnerability

**Critical Characteristics of Information**

1. Discuss the following characteristics of information:

* Availability
* Accuracy
* Authenticity
* Confidentiality
* Data owners
* Data custodians
* Data users
* Integrity
* Utility
* Possession
* Privacy

**Security Models**

1. Introduce the term **C.I.A. triad**. Use Figure 1-3 to aid the discussion.
2. Note that the definition of information security presented earlier in this chapter is based in part on a document called the U.S. National Training Standard for Information Security Professionals NSTISSI No. 4011, which was published by the U.S. Committee on National Security Systems (CNSS).
3. Introduce the term **McCumber Cube**. Use Figure 1-4 to aid the discussion.

**Balancing Information Security and Access**

1. Point out that in order to operate an information system to the satisfaction of the user and the security professional, the level of security must allow reasonable access, yet protect against threats.

**Business Needs First**

1. Discuss the important organizational functions performed by an information system.
2. The following topics should be discussed:

* **Protecting the Functionality of an Organization:** Note that the management of information security to protect an organization’s ability to function has more to do with policy and enforcement than with the technology of its implementation.
* **Enabling the Safe Operation of Applications**: Because the majority of a business’s critical data resides in complex IT applications, today’s organizations are under immense pressure to acquire and operate integrated, efficient, and capable applications.
* **Protecting Data that Organizations Collect and Use**: An important point to make is that protecting data in motion and data at rest are both critical aspects of information security. The value of data motivates attackers to steal, sabotage, or corrupt it.
* **Safeguarding Technology Assets in Organizations**: Note that in order to perform effectively, organizations must add secure infrastructure services matching the size and scope of the enterprise assets.

**Quick Quiz 1**

1. The term \_\_\_\_ refers to the organizational resource that is being protected.

Answer: asset

1. The term \_\_\_\_ refers to an intentional or unintentional act that can cause damage to or otherwise compromise the information and/or the systems that support it.

Answer: attack

1. The term \_\_\_\_ refers to a condition or state of being exposed. In information security, exposure exists when a vulnerability known to an attacker is present.

Answer: exposure

1. The term \_\_\_\_ refers to the probability that something unwanted will happen.

Answer: risk

**Threats to Information Security**

1. To understand the wide range of threats that pervade the interconnected world, researchers have interviewed practicing information security personnel and examined the information security literature on threats. Use Table 1-1 to aid the discussion.

**Common Threats**

1. Use the list on Pages 11-12 to discuss common security threats.

**Attacks on Information Security**

1. Point out that unlike threats, which are always present, attacks occur through specific actions that may cause a business loss. Use examples to aid the discussion.

**Malicious Code**

1. Use Table 1-2 to discuss the six categories of known attack vectors.

**Password Attacks**

1. Introduce the term **password cracking**.
2. The following topics should be discussed:

* **Rainbow Tables**: A rainbow attack is used when a copy of the hash of the user’s password has been obtained. When a match is found, the password has been cracked.
* **Brute Force Attacks**: Defenses against brute force attacks are usually adopted early on in any security effort and are thoroughly covered in the SANS/FBI list of the Top 20 Most Critical Internet Security Vulnerabilities.
* **Dictionary**: This attack narrows the field by selecting specific target accounts and using a list of commonly used passwords (the dictionary) instead of random combinations.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | For an interesting article on brute force attacks against WordPress sites, visit: <http://blog.sucuri.net/2012/03/brute-force-attacks-against-wordpress-sites.html> |

**Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks**:

1. Introduce the terms **distributed denial-of-service (DDoS)** and **zombies (bots)**. Use Figure 1-5 to aid the discussion.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | For an interesting article on a password attack on LinkedIn, visit: <http://money.cnn.com/2012/06/06/technology/linkedin-password-hack/index.htm> |

**Spoofing**

1. Spoofing is a technique used to gain unauthorized access to computers, wherein the intruder sends messages whose IP addresses indicate to the recipient that the messages are coming from a trusted host. Use Figure 1-6 to aid the discussion.

**Man-in-the-Middle Attacks**

1. In the well-known man-in-the-middle attack, an attacker monitors (or sniffs) packets from the network, modifies them using IP spoofing techniques, and inserts them back into the network, allowing the attacker to eavesdrop as well as to change, delete, reroute, add, forge, or divert data. Use Figure 1-7 to aid the discussion.

**E-Mail Attacks**

1. A number of attacks focus on the use of e-mail to deny service to the user (a form of DoS), exploit the inexperience or vulnerability of the user, or trick the user into installing backdoors or viruses. In general, e-mail is more the vehicle for the attack than the attack itself.
2. The following topics should be discussed:

* **Spam**: This has been used as a means of making malicious code attacks more effective. In some cases, malicious code is embedded in files that are included as attachments to spam.
* **Mail Bomb**: Another form of e-mail attack is a mail bomb, in which an attacker routes large quantities of e-mail to the target system. This can be accomplished through social engineering or by exploiting various technical flaws in the Simple Mail Transport Protocol (SMTP).

**Sniffers**

1. Explain that a sniffer is a program or device that monitors data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information from a network.

**Social Engineering**

1. Explain that within the context of information security, social engineering is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker. This can be done in several ways, and usually involves the perpetrator posing as a person higher in the organizational hierarchy than the victim.
2. Point out that the Advance Fee Fraud (AFF), internationally known as the “419” fraud, is an example of a social engineering attack. Named after a section of the Nigerian penal code, these schemes often involve fictitious companies, such as the Nigerian National Petroleum Company, but the perpetrators may invent other entities as well—a bank, a government agency, or a nongovernmental organization, such as a lottery corporation.

**Buffer Overflow**

1. A buffer overflow is an application error that occurs when more data is sent to a buffer than it can handle. Note that during a buffer overflow, the attacker can make the target system execute instructions, or the attacker can take advantage of some other unintended consequence of the failure.

**Timing Attacks**

1. Explain that the timing attack works by measuring the time required to access a Web page and deducing that the user has visited the site before by the presence of the page in the browser’s cache.

**Quick Quiz 2**

1. \_\_\_\_ are software programs that reveal their designed behavior only when activated, often appearing benign until that time.

Answer: Trojan horses

1. The term \_\_\_\_ refers to malicious software designed to operate with administrative access while hiding itself from the operating system and monitoring tools.

Answer: rootkit

1. \_\_\_\_ are hackers of limited skill who use expertly written software to attack a system.

Answer: Script kiddies

1. \_\_\_\_, the most common IP breach, is the unlawful use or duplication of software-based intellectual property.

Answer: Software piracy

**Security Professionals and the Organization**

1. Use the following sections to describe the various positions that information security professionals hold in a typical organization.

**Executive Management**

1. Introduce the terms **chief information officer (CIO)** and **chief information security officer (CISO)**.

**Information Security Project Team**

1. The information security project team consists of a number of individuals who are experienced in one or more facets of the vast array of required technical and nontechnical areas. Note that many of the same skills needed to manage and implement security are needed to design the security system.

**Information Security Policy, Standards, and Practices**

1. Introduce the terms **policy**, **standards**, **de facto standards**, and **de jure standards**. Use Figure 1-8 to aid the discussion.
2. Because information security is primarily a management problem, not a technical one, high quality security programs begin and end with policy. Point out that policy obliges personnel to function in a manner that adds to the security of information assets rather than threatens them.
3. Note that for a policy to be effective and legally enforceable, it must meet the following criteria:

* Dissemination (distribution)
* Review (reading)
* Comprehension (understanding)
* Compliance (agreement)
* Uniformity (equality of application)

1. Introduce the terms **mission**, **vision**, **strategic planning**, **security policy**, and **information security policy**.

**Enterprise Information Security Policy (EISP)**

1. Introduce the term **enterprise information security policy (EISP)**.
2. The EISP guides the development, implementation, and management of the security program. It specifies the requirements to be met by the information security blueprint or framework.
3. The following topic should be discussed:

* **EISP Components**: Although the specifics of EISPs vary from organization to organization, most EISP documents include the components shown in Table 1-3.

**Issue-Specific Security Policy (ISSP)**

1. As an organization executes various technologies and processes to support routine operations, it must instruct employees on the proper use of those technologies and processes. Explain that the issue-specific security policy (ISSP), which requires frequent updates, addresses specific areas of technology, stating the organization’s position on each issue. Use Table 1-4 to aid the discussion.

**Systems-Specific Policy (SysSP)**

1. Note that whereas issue-specific policies are written documents readily identifiable as policy, system specific security policies (SysSPs) sometimes have a different look. They can be separated into two general areas, managerial guidance and technical specifications, or they can be combined into a single policy document.
2. The following topics should be discussed:

* **Managerial Guidance SysSPs**: A managerial guidance SysSP document is created by management to guide the implementation and configuration of technology, as well as to regulate the behavior of people in the organization.
* **Technical Specifications SysSPs**: Introduce the terms **access control lists (ACLs)**, **capability table, access control matrix**, and **configuration rule policies**.

**Frameworks and Industry Standards in Information Security**

1. Introduce the terms **security blueprint** and **security framework**.
2. To select a methodology by which to develop an information security blueprint, you can adapt or adopt a published information security model or framework. Note that this framework can be an outline of steps to take to design and implement information security in the organization.

**The ISO 27000 Series**

1. One of the most widely referenced security models is Information Technology - Code of Practice for Information Security Management, which was originally published as British Standard 7799. In 2000, this code of practice was adopted as an international standard framework for information security by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as ISO/IEC 17799 (or more commonly just ISO 17799). Use Tables 1-5 and 1-6, and Figure 1-9 to aid the discussion.

**NIST Security Models**

1. Another approach to security standards is described in documents available from the Computer Security Resource Center of the National Institute for Standards and Technology (csrc.nist.gov). Discuss the NIST documents that can assist in the design of a security framework.

**IETF Security Architecture**

1. Note that the Security Area Working Group acts as an advisory board for the protocols and areas developed and promoted by the Internet Society and the Internet Engineering Task Force (IETF), and although the group endorses no specific information security architecture, one of its requests for comment, RFC 2196: *Site Security Handbook*, offers a good discussion of important security issues.

**Benchmarking and Best Business Practices**

1. Benchmarking and best practices are methods used by some organizations to assess security practices. They do not provide a complete methodology for the design and implementation of all the practices needed by an organization; however, it is possible to formulate the desired outcome of the security process and work backwards toward an effective design. Introduce the Federal Agency Security Practices (FASP) Web site and discuss other public and private institutions provide information on best practices.
2. The following topics should also be discussed:

* **Spheres of Security**: The spheres of security, shown in Figure 1-10, are the foundation of the security framework. Generally speaking, they illustrate that information is under attack from a variety of sources.
* **Defense in Depth**: One of the basic tenets of security architectures is the layered implementation of security. This layered approach is called defense in depth. To achieve defense in depth, an organization must establish multiple layers of security controls and safeguards, which can be organized into policy, training and education, and technology per the NSTISSC model. Introduce the term **redundancy** and use Figure 1-11 to aid the discussion.
* **Security Perimeter**: A security perimeter defines the boundary between the outer limit of an organization’s security and the beginning of the outside world. Note that a security perimeter protects all internal systems from outside threats, as shown in Figure 1-12. Introduce the term **security domains**.

**Quick Quiz 3**

1. The \_\_\_\_ is often the senior technology officer. Titles such as vice president (VP) of information, VP of information technology, and VP of systems may also be used.

Answer: chief information officer (CIO)

1. The \_\_\_\_ is the individual primarily responsible for the assessment, management, and implementation of information security in the organization.

Answer: chief information security officer (CISO)

1. \_\_\_\_ is the process of moving the organization towards its vision.

Answer: Strategic planning

1. A(n) \_\_\_\_ provides rules for the protection of the information assets of the organization.

Answer: information security policy

# **Class Discussion Topics**

1. What motivates a cyberactivist to do what he/she does?
2. Are cyberactivists cyber criminals?

# **Additional Projects**

Using the Internet as a resource, submit a report that discusses at least five emerging threats to information security.

Submit a report that provides guidelines for creating strong passwords.

# **Additional Resources**

1. Home Network Security: <http://www.cert.org/tech_tips/home_networks.html>
2. 2012 Security Predictions: <http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2012.pdf>
3. Social Engineering: <http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics>
4. Social Engineering: <http://www.sans.org/reading_room/whitepapers/privacy/disney-princess-you_33328>

**Key Terms**

* **access control matrix** A combination of access control list information, which specifies users’ rights on an asset, and capability table information, which specifies asset rights for a particular user.
* **access** The ability to use, manipulate, modify, or affect an asset or resource.
* **accuracy** A characteristic of information in which it is free from mistakes or errors and has the value that the end user expects it to have.
* **asset** An organizational resource that has value to the organization. In information security, this is often the resource that is being protected.
* **attack** An act or action that takes advantage of a vulnerability to compromise a controlled system using intentional or unintentional steps that can cause damage or loss.
* **authenticity** A characteristic of information in which it is in a quality or state of being genuine or original rather than a reproduction or fabrication.
* **availability** A characteristic of information in which authorized users—persons or computer systems—have access to information without interference or obstruction and are able to receive it in the required format.
* **backdoor** A hidden opening in a system that could allow viruses, Trojan horses, or hackers to access the system at will, bypassing standard forms of authentication.
* **boot virus** A form of computer virus that infects the key operating system files located in a computer’s boot sector.
* **bot** Short for “robot,” a malicious code capability in a virus or worm that implies that the computer is infested and is under another entity’s control.
* **brute force attack** A form of password guessing attack that uses computing and network resources to try every possible combination of available characters, numbers, and symbols for a password.
* **buffer overflow** An application error that occurs when more data is sent to a buffer than it can handle, possibly resulting in the targeted system executing unintended instructions or performing some other unauthorized action.
* **capability table** A list of authorization rights associated with a user—in other words, what information assets the user can access and what the user can do with them.
* **chief information officer (CIO)** The member of an organization’s management team (often the senior technology officer) who is in charge of all information systems.
* **chief information security officer (CISO)** The member of an organization’s management team who is primarily responsible for the assessment, management, and implementation of information security.
* **communications security** The protection of an organization’s communications media, technology, and content.
* **computer viruses** Segments of code that perform malicious actions, including macro viruses and boot viruses.
* **confidentiality** A characteristic of information in which it is limited or restricted to authorized individuals or systems and thus protected from disclosure or exposure.
* **configuration rule policies** The specific instructions entered into a security system to regulate how it reacts to the data it receives.
* **control**  Security mechanisms, policies, or procedures that can successfully counterattack, reduce risk, resolve vulnerabilities, and otherwise improve the security within an organization.
* **cracker** An individual who “cracks” or removes software protection that is designed to prevent unauthorized duplication or use.
* **cyberterrorist** An individual or group that bypasses legitimate system controls so as to conduct terrorist (or, more often, terrorist-like) activities using technical or social engineering means.
* **data custodians** Those who work directly with data owners and are responsible for the storage, maintenance, and protection of the information.
* **data owners** Those who are responsible for the security and use of a particular set of information.
* **data users** The end users who work with the information to perform their daily jobs supporting the mission of the organization.
* **defense in depth** A strategic approach to security in which multiple, concentric control options are implemented to ensure that the failure of one, or even several, control layers does not result in a loss to an asset.
* **denial-of-service (DDoS)** An attack against a network based asset in which the attacker sends a large number of otherwise innocuous requests to a target, thus keeping it from being able to perform its primary function for legitimate users.
* **dictionary attack** A form of password guessing attack that narrows the field for guesses by selecting specific target accounts and using a list of commonly used passwords (the dictionary) instead of random combinations.
* **distributed denial-of-service (DDoS)**  A variant of the denial-of-service attack against a network-based asset in which multiple and geographically disbursed sources of attack (often bots being controlled by others) are used to deny service to legitimate users of a service or system by overloading the target with otherwise innocuous requests.
* **exploit** A technique used to compromise a system.
* **exposure** A condition or state of being exposed. In information security, exposure exists when a vulnerability known to an attacker is present.
* **guessing attack** Attempt to bypass access controls by guessing passwords.
* **hackers** Individuals who gain access, often illegally, to information or systems without explicit authorization.
* **Hacktivist (cyberactivist)** An individual (sometimes a group) who interferes with or disrupts systems to protest the operations, policies, or actions of an organization or government agency.
* **information security policy** A set of rules that provides for the protection of the information assets of the organization.
* **integrity** A characteristic of information when it is whole, complete, and uncorrupted.
* **intellectual property** The product of creative thought and other activities of the mind, such as invention, literature, art, logos, names, symbols, and other creative works.
* **loss** The instance of an information asset suffering damage, unintended or unauthorized modification, or disclosure.
* **macro virus** A form of computer virus that is embedded in the automatically executing macro code common in word processors, spread sheets, and database applications.
* **mail bomb** A form of e-mail attack in which an attacker routes large quantities of e-mail to the target system to effect a denial of use for legitimate users.
* **malicious code (malcode)** Software components or programs designed to damage, destroy, or deny service to the target systems; it includes viruses, worms, Trojan horses, and an expanding taxonomy of other malicious software.
* **managerial guidance SysSP** A form of system-specific policy created by management to guide the implementation and configuration of technology as well as to regulate the behavior of people in the organization.
* **man-in-the-middle attack** An attack technique used to gain unauthorized access to computers wherein an attacker monitors (or sniffs) packets from the network, modifies them using IP spoofing techniques, and inserts them back into the network, allowing the attacker to eavesdrop as well as to change, delete, reroute, add, forge, or divert data.
* **McCumber Cube** A graphical description of the architectural approach widely used in computer and information security, consisting of a representation of a 3 x 3 x 3 cube in which the 27 cells represent areas that must be addressed to secure information systems.
* **mission** A written statement of an organization’s purpose.
* **network security** The protection of networking components, connections, and contents, which is the primary focus of this textbook.
* **operations security** The protection of the details of a particular operation or series of activities.
* **packet monkeys** A class of script kiddie hackers who use automated tools to inundate a Web site with a barrage of network traffic, usually resulting in a denial of service.
* **password cracking** An attempt to bypass access controls by guessing passwords.
* **personal security** The protection of those who are authorized to access an organization and its operations.
* **phreaker** A class of hackers who attack the public telephone network to make free calls or disrupt services.
* **physical security** The protection of the physical items or areas of an organization from unauthorized access and misuse.
* **policy** (1) Guidance or instructions that an organization’s senior management implements to regulate the activities of the organization members who make decisions, take actions, and perform other duties. (2) Specific instructions or configurations in a computer system that define the actions permissible by users of that system.
* **possession** The ownership or control of some object or item.
* **privacy** A characteristic of information that is used in accordance with the legal requirements mandated for employees, partners, and customers.
* **protection profile** 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.
* **rainbow attack** A form of password guessing attack that uses a database of precomputed hashes (or rainbow tables) derived from sequentially calculated passwords to look up the hashed password and derive the plaintext version.
* **rainbow tables** A database of precomputed hashes derived from sequentially calculated passwords to look up the hashed password and read out the text version.
* **redundancy** The process of planning for duplicate service capabilities, usually to improve availability in the event of a failure of a device or service.
* **risk** The probability that something unwanted will happen.
* **Rootkit** A form of malicious software designed to operate with administrative access while hiding itself from the operating system and monitoring tools.
* **script kiddies** A class of hackers of limited skill who use expertly written software to attack a system.
* **security blueprint** The basis for the design, selection, and implementation of all security program elements; it is a detailed version of the security framework.
* **security domains** Areas of trust within which users can freely communicate without the need to authenticate repeatedly.
* **security framework** An outline of the overall information security strategy and a roadmap for planned changes to the organization’s information security environment.
* **security perimeter** The boundary between the outer limit of an organization’s security and the beginning of the outside world.
* **shoulder surfing** A process of observing others’ passwords by watching system login activities.
* **sniffer** A program or device that monitors data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information from a network.
* **social engineering** A process of using social skills to convince system users to reveal access credentials or other valuable information to the attacker, which enables an attack or loss to the system.
* **software piracy** The unlawful use or duplication of software-based intellectual property.
* **spam** Unsolicited commercial e-mail that is sometimes used as a means of making malicious code attacks more effective.
* **spoofing** An attack technique used to gain unauthorized access to computers, wherein the intruder sends messages whose IP addresses indicate to the recipient that the messages are coming from a trusted host.
* **standards** Detailed descriptions of what must be done to comply with policy.
* **strategic planning** A process of moving the organization towards its vision by identifying means and methods to accomplish change.
* **technical specifications SysSP** A form of system-specific policy designed to guide the technical configuration of a control; these are often access control lists or configuration rule policies.
* **threat** A category of objects, persons, or other entities that presents a danger to an asset.
* **threat agent** The specific instance of a threat or a particular component of a threat.
* **timing attack** A means of attack that uses a measure of elapsed time to deduce useful information about what is happening out of site. An attack method whereby the attacker eavesdrops on the victim’s session and uses statistical analysis of patterns and inter-keystroke timings to discern sensitive session information.
* **Trojan horses** Software programs that reveal their designed behavior only when activated, often appearing benign until that time.
* **utility** A characteristic of information that describes the information as having value for some purpose or end.
* **vision** A written statement of an organization’s long-term goals.
* **vulnerability** Weaknesses or faults in a system or protection mechanism that open it to the possibility of attack or damage.
* **worms** Malicious programs that replicate themselves without requiring another program to provide a safe environment for replication.