Chapter 2: The Need for Security

Overview

This chapter examines the business drivers behind the information security analysis design process. It examines current organizational and technological security needs, and emphasizes and builds on the concepts presented in the previous chapter. This chapter also examines the various threats facing organizations and present methods for ranking these threats that organizations can use when they begin their security planning process.

Learning Objectives

Upon completion of this material, you should be able to:

- Demonstrate that organizations have a business need for information security
- Explain why a successful information security program is the responsibility of both an organization's general management and IT management
- Identify the threats posed to information security and the more common attacks associated with those threats, and differentiate threats to the information within systems form attacks against the information within systems
- Describe the issues facing software developers, as well as the common errors made by developers, and explain how software development programs can create software that is more secure and reliable.

Business Needs First

There are four (4) important functions of an organization that the information security performs:

1. Protecting the organization's ability to function
2. Enabling the safe operation of applications running on the organization's IT systems
3. Protecting the data the organization collects and uses
4. Safeguarding the organization's technology assets

Protecting the Functionality of an Organization

- Shared responsibility between general management and IT management.
    - Set security policy in compliance with legal requirements.
    - Not really a technology issue.
- Address information security in terms of
    - Business impact
    - Cost of business interruption

Enabling Safe Operating of Applications

- Operation requires integrated, efficient, and capable applications.
- A modern organization needs to create an environment that protect critical applications such as
    - Operating system platforms
    - Electronic mail
    - Instant messaging
- These can be acquired by outsourcing to a service provider or can be developed internally.

- Protection of the infrastructure must be overseen by management.

Protecting Data that Organizations Collect and Use

- Data provides
  - Record of transactions (e.g. banking)
  - Ability to deliver value to customers
  - Enable creation and movement of goods and services
- Information systems and the data they process enable the creation and movement of goods and services.
- Therefore, protecting **data in motion** (online transactions) and **data at rest** (offline transactions) are both critical aspects of information security.
- An effective information security program implemented by management protects the integrity and value of the organization's data.

Safeguarding Technology Assets in Organizations

- Organizations must have secure infrastructure services based on the size and scope of the enterprise.
  - Smaller businesses may require less protections such as email service provided by an ISP and augmented with a personal encryption tool.
  - Additional services are required for larger businesses such as Public Key Infrastructure (PKI), an integrated system of software, encryption methodologies, and legal agreements that can be used to support the entire information infrastructure.
- In general, as an organization's network grows to accommodate changing needs, more robust technology solutions should replace security programs the organization has outgrown.

Threats

500 B.C. – Chinese general Sun Tzu Wu wrote *The Art of War*, a military treatise that emphasizes the importance of knowing yourself as well as the threats you face.

To protect your organization's information, you must:

1. Know yourself; that is, be familiar with the information to be protected and the systems that store, transport, and process it; and
2. Know the threats you face.

Threat – is an object, person, or entity that represents a constant danger to an asset.

14 Categories of Threat

There are 14 categories of threat, which is discussed below.

1. Compromises to Intellectual Property

Intellectual Property – defined as "the ownership of ideas and control over the tangible or virtual representation of those ideas. Use of another person's intellectual property may or may not involve royalty payments or permission, but should always include proper credit to the source." These can be trade secrets, copyrights, trademarks, and patents.

Software piracy – Unlawful use or duplication of software-based intellectual property. It is also the most common IP breach.

A number of technical mechanisms have been used to enforce copyright law. This includes

- Digital watermarks and embedded code
- Copyright codes
- Intentional placement of bad sectors on software media

License agreement – a window that usually pops up during the installation of new software. This is the most common tool used to establish that the user has read and agrees to the license agreement.

Online registration process – Another effort to combat piracy. Individuals who install software are often asked or even required to register their software to obtain technical support or the use of all features.

2. Deliberate Software Attacks

Deliberate software attacks occur when an individual or group designs and deploys software to attack a system.

Malicious code (sometimes known as **malicious software** or **malware**) – software components or programs designed to damage, destroy, or deny service to the target systems. The following are some common instances of malicious code.

1. **Virus –** a computer virus is designed to spread from host to host and has the ability to replicate itself. Similarly, in the same way that the flu viruses cannot reproduce without a host cell, computer viruses cannot reproduce and spread without programming such as a file or document. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code. In the process, a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data. (What Is A Computer Virus?, 2020).

2. **Worm -** A computer worm is a type of malware that spreads copies of itself from computer to computer. A worm can replicate itself without any human interaction, and it does not need to attach itself to a software program in order to cause damage. Worms can modify and delete files, and they can even inject additional malicious software onto a computer. Sometimes a computer worm's purpose is only to make copies of itself over and over — depleting system resources, such as hard drive space or bandwidth, by overloading a shared network. In addition to wreaking havoc on a computer's resources, worms can also steal data, install a backdoor, and allow a hacker to gain control over a computer and its system settings. (What is a computer worm and how does it work?, 2019).

3. **Trojan Horses -** A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems. Once activated, Trojans can enable cyber-criminals to spy on you, steal your sensitive data, and gain backdoor access to your system. These actions can include deleting data, blocking data, modifying data, copying data, and disrupting the performance of computers or computer networks. (Kaspersky, 2019)

4. **Back Door** or **Trap Door –** A virus or worm can have a payload that installs a **back door** or **trap door** component in a system, which allows the attacker to access the system at will with special privileges. Examples of these kinds of payloads include Subeven and Back Orifice.

5. **Polymorphic Threats** – A polymorphic threat is one that over time changes the way it appears to antivirus software programs, making it undetectable by techniques that look for preconfigured signatures. These viruses and worms actually evolve, changing their size and other external file characteristics to elude detection by antivirus software programs.

6. **Virus and Worm Hoaxes –** These are messages with false warning about a computer virus or worm. Typically, the warning arrives in an e-mail note or is distributed through a note in a company's internal network. These notes are usually forwarded using distribution lists and they will typically suggest that the recipient forward the note to other distribution lists. (TechTarget Contributors, 2017).

3. Deviations in Quality of Service

Companies rely on a number of service providers: power, water, sewage, internet, and phone, just to name a few. If one of these providers has irregular service, it could disrupt business operations and threaten the security of information. We refer to this condition as an availability disruption and interruption in service, usually from a service provider, which can cause an adverse event within the organization.

1. **Power –** One of the most important services to the organization's IT equipment is electrical power. Too much or not enough power can cause major issues with computer equipment. Some common conditions include:
    a. **Blackout** – long-term interruption or outage in electrical power availability.
    b. **Brownout –** a long-term decrease in the quality of electrical power availability.
    c. **Fault –** a short-term interruption in electrical power availability.
    d. **Noise –** the presence of additional and disruptive signals in network communications or electrical power delivery.
    e. **Sag –** a short-term decrease in electrical power availability.
    f. **Spike –** a short term increase in electrical power availability.
    g. **Surge –** a long-term increase in electrical power availability.

2. **Internet –** Many organizations today rely heavily on their Internet and web services to both communicate with supplier and clients, and to acquire and deliver products and services. A failure of this connection would negatively impact the organization. Specific threats or attacks to this connection involve both physical disruptions, like a contractor digging up a cable, or a tree falling on a line, as well as electronic disruptions. Many electrical disruptions, intentional, or accidental, cover multiple threat categories.

    In order to minimize the impact and probability of availabilities disruptions, we expect documented commitment from our service providers that they will provide quality service or provide some form of restitution should they fail. The document that specifies the expected level of service from a service provider is known as a **Service Level Agreement**, or **SLA**. An SLA usually contains provisions for a minimum acceptable availability and penalties for remediation procedures for downtime.

3. **Communications and Other Service Provider Issues –** Other utility services can affect organizations as well. Among these are telephone, water, wastewater, trash pickup, cable television, natural or propane gas, and custodial services. The loss of these services can impair the ability of an organization to function. For instance, most facilities require water service to operate an air-conditioning system. If a wastewater system fails, an organization might be prevented from allowing employees into the building.

4. Espionage or Trespass

Espionage or trespass is a well-known and broad category of electronic and human activities that can breach the confidentiality of information. When an unauthorized individual gains access to the information an organization is trying to protect, data is categorized as espionage or trespass. Attackers can use many different methods to access the information stored in an information system. Some information gathering techniques are quite legal, for example, using a web browser to perform market research. These legal techniques are called, collectively, competitive intelligence. When an information gatherers employ techniques that cross the threshold what is legal or ethical, they are conducting industrial espionage.
Acts of **trespass** can lead to an authorized real our virtual actions that enable information gatherers to enter premises or systems they have not pin authorized to enter. Controls sometimes mark the boundaries of an organization's virtual territory. These boundaries give notice to trespassers that they are encroaching on the organization's cyberspace. Sound principles of authentication and authorization can help organizations protect valuable information and systems. This control methods and methodologies employ multiple layers or factors to protect against unauthorized access.

Forms of espionage include:

1. **Shoulder surfing -** this technique is used in public or semipublic settings when individuals gather information that they are not authorized so have by looking over another individual's shoulder or viewing the information from a distance. Instances of shoulder surfing occur at computer terminals, desks, ATM machines, on the bus for subway where people use smartphones and tablet PCs, or other places where a person is accessing confidential information.

2. **Hackers** - these are "people who use and create computer software to gain access to information illegally." Hackers are frequently glamorized in fictional accounts as people who stealthily manipulate a maze of computer networks, systems, and data to find the information that solves the mystery or saves the day.

3. **Phreaker -** A phreaker hacks the public telephone network to make free calls or disrupt services. Phreakers grew in fame in the 1970s when they developed devices called blue boxes that enabled free calls from pay phones. Later, red boxes were developed to simulate the tones of coins falling in a pay phone, and finally black boxes emulated the line voltage. With the advent of digital communications, these boxes became practically obsolete. Even with the loss of the colored box technologies, phreakers continue to cause problems for all telephone systems.

5. Forces of Nature

Forces of nature, force majeure, or acts of God can present some of the most dangerous threats, because they usually occur with very little warning and are beyond the control of people. These threats, which include events such as fires, floods, earthquakes, and lightning as well as volcanic eruptions and insect infestations, can disrupt not only the lives of individuals but also the storage, transmission, and use of information. Some of the more common threats in this group are listed here.

1. **Fire -** In this context, usually a structural fire that damages a building housing computing equipment that comprises all or part of an information system, as well as smoke damage and/or water damage from sprinkler systems or firefighters. This threat can usually be mitigated with fire casualty insurance and/or business interruption insurance.

2. **Flood** - An overflowing of water onto an area that is normally dry, causing direct damage to all or part of the information system or to the building that houses all or part of the information system. A flood might also disrupt operations through interruptions in access to the buildings that house all

or part of the information system. This threat can sometimes be mitigated with flood insurance and/or business interruption insurance.

3. **Earthquake** - A sudden movement of the earth's crust caused by the release of stress accumulated along geologic faults or by volcanic activity. Earthquakes can cause direct damage to all or part of the information system or, more often, to the building that houses it, and can also disrupt operations through interruptions in access to the buildings that house all or part of the information system. This threat can sometimes be mitigated with specific casualty insurance and/or business interruption insurance, but is usually a separate policy.

4. **Lightning** - An abrupt, discontinuous natural electric discharge in the atmosphere. Lightning usually directly damages all or part of the information system an/or its power distribution components. It can also cause fires or other damage to the building that houses all or part of the information system, and disrupt operations by interfering with access to the buildings that house all or part of the information system. This threat can usually be mitigated with multipurpose casualty insurance and/or business interruption insurance.

5. **Landslide or mudslide** - The downward sliding of a mass of earth and rock directly damaging all or part of the information system or, more likely, the building that houses it. Land- or mudslides also disrupt operations by interfering with access to the buildings that house all or part of the information system. This threat can sometimes be mitigated with casualty insurance and/or business interruption insurance.

6. **Tornado or severe windstorm** - A rotating column of air ranging in width from a few yards to more than a mile and whirling at destructively high speeds, usually accompanied by a funnel-shaped downward extension of a cumulonimbus cloud. Storms can directly damage all or part of the information system or, more likely, the building that houses it, and can also interrupt access to the buildings that house all or part of the information system. This threat can sometimes be mitigated with casualty insurance and/or business interruption insurance.

7. **Hurricane or typhoon** - These storms may disrupt operations by interrupting access to the buildings that house all or part of the information system. This threat can sometimes be mitigated with casualty insurance and/or business interruption insurance.

8. **Tsunami** - A very large ocean wave caused by an underwater earthquake or volcanic eruption. These events can directly damage all or part of the information system or, more likely, the building that houses it. Organizations located in coastal areas may experience tsunamis. Tsunamis may also cause disruption to operations through interruptions in access or electrical power to the buildings that house all or part of the information system. This threat can sometimes be mitigated with casualty insurance and/or business interruption insurance.

9. **Electronic discharge (ESD)** - Usually, static electricity and ESD are little more than a nuisance. Unfortunately, however, the mild static shock we receive when walking across a carpet can be costly or dangerous when it ignites flammable mixtures and damages costly electronic components. Static electricity can draw dust into clean-room environments or cause products to stick together. The cost of ESD-damaged electronic devices and interruptions to service can range from only a few cents to several millions of dollars for critical systems. Loss of production time in information processing due to ESD impact is significant. While not usually viewed as a threat, ESD can disrupt information systems, but it is not usually an insurable loss unless covered by business interruption insurance.

10. **Dust contamination** - Some environments are not friendly to the hardware components of information systems. Because dust contamination can shorten the life of information systems or cause unplanned downtime, this threat can disrupt normal operations.

Since it is not possible to avoid force of nature threats, organizations must implement controls to limit damage, and they must also prepare contingency plans for continued operations, such as disaster recovery plans, business continuity plans, and incident response plans.

6. Human Error or Failure

This category includes acts performed without intent or malicious purpose by an authorized user. When people use information systems, mistakes happen. Inexperience, improper training, and the incorrect assumptions are just a few things that can cause these misadventures. Regardless of the cause, even innocuous mistakes can produce extensive damage.

One of the greatest threats to an organization's information security is the organization's own employees. **Employees** are the threat agents closest to the organizational data. Because employees use data in everyday activities to conduct the organization's business, their mistakes represent a serious threat to the confidentiality, integrity, and availability of data, relative to threats from outsiders.

Much human error or failure can be prevented with training and ongoing awareness activities, but also with controls, ranging from simple procedures, such as requiring the user to type a critical command twice, to more complex procedures, such as the verification of commands by a second party.

7. Information Extortion

Information extortion occurs when an attacker or trusted insider steals information from a computer system and demands compensation for its return or for an agreement not to disclose it. Extortion is common in credit card number theft.

8. Missing, Inadequate, or Incomplete Organizational Policy or Planning.

Missing, inadequate, or incomplete organizational policy or planning makes an organization vulnerable to loss, damage, or disclosure of information assets when other threats lead to attacks. Information security is, at its core, a management function. The organization's executive leadership is responsible for strategic planning for security as well as for IT and business functions—a task known as governance.

9. Missing, Inadequate, or Incomplete Controls

Missing, inadequate, or incomplete controls—that is, security safeguards and information asset protection controls that are missing, misconfigured, antiquated, or poorly designed or managed—make an organization more likely to suffer losses when other threats lead to attacks.

For example, if a small organization installs its first network using small office/home office (SOHO) equipment (which is similar to the equipment you might have on your home network) and fails to upgrade its network equipment as it becomes larger, the increased traffic can affect performance and cause information loss. Routine security audits to assess the current levels of protection help to ensure the continuous protection of organization's assets.

10. Sabotage or Vandalism

This category of threat involves the deliberate sabotage of a computer system or business, or acts of vandalism to either destroy an asset or damage the image of an organization. These acts can range from petty vandalism by employees to organized sabotage against an organization.

Although not necessarily financially devastating, attacks on the image of an organization are serious. Vandalism to a Web site can erode consumer confidence, thus diminishing an organization's sales and net worth, as well as its reputation.

There are innumerable reports of hackers accessing systems and damaging or destroying critical data. Hacked Web sites once made front-page news, as the perpetrators intended. The impact of these acts has lessened as the volume has increased.

Compared to Web site defacement, vandalism within a network is more malicious in intent and less public. Today, security experts are noticing a rise in another form of online vandalism, **hacktivist** or **cyberactivist** operations, which interfere with or disrupt systems to protest the operations, policies, or actions of an organization or government agency.

A much more sinister form of hacking is **cyberterrorism**. Cyberterrorists hack systems to conduct terrorist activities via network or Internet pathways. The United States and other governments are developing security measures intended to protect the critical computing and communications networks as well as the physical and power utility infrastructures.

11. Theft

The threat of theft—the illegal taking of another's property, which can be physical, electronic, or intellectual—is a constant. The value of information is diminished when it is copied without the owner's knowledge.

Physical theft can be controlled quite easily by means of a wide variety of measures, from locked doors to trained security personnel and the installation of alarm systems. Electronic theft, however, is a more complex problem to manage and control. When someone steals a physical object, the loss is easily detected; if it has any importance at all, its absence is noted. When electronic information is stolen, the crime is not always readily apparent. If thieves are clever and cover their tracks carefully, no one may ever know of the crime until it is far too late.

12. Technical Hardware Failures or Errors

Technical hardware failures or errors occur when a manufacturer distributes equipment containing a known or unknown flaw. These defects can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability. Some errors are terminal—that is, they result in the unrecoverable loss of the equipment. Some errors are intermittent, in that they only periodically manifest themselves, resulting in faults that are not easily repeated, and thus, equipment can sometimes stop working, or work in unexpected ways.

13. Technical Software Failures or Errors

Large quantities of computer code are written, debugged, published, and sold before all their bugs are detected and resolved. Sometimes, combinations of certain software and hardware reveal new bugs. These failures range from bugs to untested failure conditions. Sometimes these bugs are not errors, but rather purposeful shortcuts left by programmers for benign or malign reasons. Collectively, shortcut access routes into programs that bypass security checks are called trap doors and can cause serious security breaches.

14. Technological Obsolescence

Antiquated or outdated infrastructure can lead to unreliable and untrustworthy systems. Management must recognize that when technology becomes outdated, there is a risk of loss of data integrity from attacks.

Management's strategic planning should always include an analysis of the technology currently in use. Ideally, proper planning by management should prevent technology from becoming obsolete, but when obsolescence is manifest, management must take immediate action. IT professionals play a large role in the identification of probable obsolescence.

Attacks

An **attack** is an act that takes advantage of a vulnerability to compromise a controlled system. It is accomplished by a **threat agent** that damages or steals an organization's information or physical asset.

A **vulnerability** is an identified weakness in a controlled system, where controls are not present or are no longer effective. Unlike threats, which are always present, attacks only exist when a specific act may cause a loss.

The following are the major types of attacks used against controlled systems:

1. Malicious Code

The **malicious code** attack includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information. The state-of-the-art malicious code attack is the polymorphic, or multivector, worm. These attack programs use up to six known attack vectors to exploit a variety of vulnerabilities in commonly found information system devices.

Other forms of malware include covert software applications—bots, spyware, and adware— that are designed to work out of sight of users or via an apparently innocuous user action.

- A **bot** (an abbreviation of robot) is an automated software program that executes certain commands when it receives a specific input. Bots are often the technology used to implement Trojan horses, logic bombs, back doors, and spyware.
- **Spyware** is "any technology that aids in gathering information about a person or organization without their knowledge. Spyware is placed on a computer to secretly gather information about the user and report it. The various types of spyware include:
    - a Web bug, a tiny graphic on a Web site that is referenced within the Hypertext Markup Language (HTML) content of a Web page or e-mail to collect information about the user viewing the HTML content;
    - a tracking cookie, which is placed on the user's computer to track the user's activity on different Web sites and create a detailed profile of the user's behavior.
- **Adware** is any software program intended for marketing purposes such as that used to deliver and display advertising banners or popups to the user's screen or tracking the user's online usage or purchasing activity.

2. Hoaxes

A more devious attack on computer systems is the transmission of a virus hoax with a real virus attached. When the attack is masked in a seemingly legitimate message, unsuspecting users more readily distribute it. Even though these users are trying to do the right thing to avoid infection, they end up sending the attack on to their coworkers and friends and infecting many users along the way.

3. Back Doors

Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource through a back door. Sometimes these entries are left behind by system designers or maintenance staff, and thus are called trap doors. A trap door is hard to detect, because very often the programmer who puts it in place also makes the access exempt from the usual audit logging features of the system.

4. Password Crack

Attempting to reverse-calculate a password is often called **cracking**. A cracking attack is a component of many dictionary attacks. It is used when a copy of the Security Account Manager (SAM) data file, which contains hashed representation of the user's password, can be obtained. A password can be hashed using the same algorithm and compared to the hashed results. If they are the same, the password has been cracked.

5. Brute Force

The application of computing and network resources to try every possible password combination is called a **brute force attack**. Since the brute force attack is often used to obtain passwords to commonly used accounts, it is sometimes called a password attack. If attackers can narrow the field of target accounts, they can devote more time and resources to these accounts. That is one reason to always change the manufacturer's default administrator account names and passwords.

6. Dictionary Attack

The dictionary attack is a variation of the brute force attack which narrows the field by selecting specific target accounts and using a list of commonly used passwords (the dictionary) instead of random combinations. Organizations can use similar dictionaries to disallow passwords during the reset process and thus guard against easy-to-guess passwords. In addition, rules requiring numbers and/or special characters in passwords make the dictionary attack less effective.

7. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS)

In a **denial-of-service** (**DoS**) attack, the attacker sends a large number of connection or information requests to a target. So many requests are made that the target system becomes overloaded and cannot respond to legitimate requests for service. The system may crash or simply become unable to perform ordinary functions.

A **distributed denial-of- service** (**DDoS**) is an attack in which a coordinated stream of requests is launched against a target from many locations at the same time. Most DDoS attacks are preceded by a preparation phase in which many systems, perhaps thousands, are compromised. The compromised machines are turned into **zombies**, machines that are directed remotely (usually by a transmitted command) by the attacker to participate in the attack.

8. Spoofing

Spoofing is a technique used to gain unauthorized access to computers, wherein the intruder sends messages with a source IP address that has been forged to indicate that the messages are coming from a trusted host. To engage in IP spoofing, hackers use a variety of techniques to obtain trusted IP addresses, and then modify the packet headers to insert these forged addresses. Newer routers and firewall arrangements can offer protection against IP spoofing.

9. Man-in-the-Middle

In the well-known **man-in-the-middle** or **TCP hijacking attack**, an attacker monitors (or sniffs) packets from the network, modifies them, and inserts them back into the network. This type of attack uses IP spoofing to enable an attacker to impersonate another entity on the network. It allows the attacker to eavesdrop as well as to change, delete, reroute, add, forge, or divert data. A variant of TCP hijacking, involves the interception of an encryption key exchange, which enables the hacker to act as an invisible man-in-the-middle—that is, an eavesdropper—on encrypted communications.

10. Spam

Spam is unsolicited commercial e-mail. While many consider spam a trivial nuisance rather than an attack, it has been used as a means of enhancing malicious code attacks. The most significant consequence of spam, however, is the waste of computer and human resources. Many organizations attempt to cope with the flood of spam by using e-mail filtering technologies. Other organizations simply tell the users of the mail system to delete unwanted messages.

11. Mail Bombing

Another form of e-mail attack that is also a DoS is called a **mail bomb**, in which an attacker routes large quantities of e-mail to the target. This can be accomplished by means of social engineering or by exploiting various technical flaws in the Simple Mail Transport Protocol (SMTP). The target of the attack receives an unmanageably large volume of unsolicited e-mail. By sending large e-mails with forged header information, attackers can take advantage of poorly configured e-mail systems on the Internet and trick them into sending many e-mails to an address chosen by the attacker. If many such systems are tricked into participating in the event, the target e-mail address is buried under thousands or even millions of unwanted e-mails.

12. Sniffers

A **sniffer** is a program or device that can monitor data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information. Unauthorized sniffers can be extremely dangerous to a network's security, because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favorite weapon in the hacker's arsenal. Sniffers often work on TCP/IP networks, where they're sometimes called packet sniffers. Sniffers add risk to the network, because many systems and users send information on local networks in clear text. A sniffer program shows all the data going by, including passwords, the data inside files—such as word-processing documents—and screens full of sensitive data from applications.

13. Social Engineering

Social engineering is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker. There are several social engineering techniques, which usually involve a perpetrator posing as a person higher in the organizational hierarchy than the victim. To prepare for this false representation, the perpetrator may have used social engineering tactics against others in the organization to collect seemingly unrelated information that, when used together, makes the false representation more credible.

14. Phishing

Phishing is an attempt to gain personal or financial information from an individual, usually by posing as a legitimate entity. Phishing attacks use three primary techniques, often in combination with one another: URL manipulation, Web site forgery, and phone phishing.

- **URL manipulation**, attackers send an HTML embedded e-mail message, or a hyperlink whose HTML code opens a forged Web site.

- In the **forged Web site**, phishers publish a website by copying the design, content, and user interface of a legitimate website.
- **Phone phishing** is pure social engineering. The attacker calls a victim on the telephone and pretends to be someone they are not (a practice sometimes called pretexting) in order to gain access to private or confidential information such as health or employment records or financial information. They may impersonate someone who is known to the potential victim only by reputation.

15. Pharming

Pharming is the redirection of legitimate Web traffic (e.g., browser requests) to an illegitimate site for the purpose of obtaining private information. Pharming often uses Trojans, worms, or other virus technologies to attack the Internet browser's address bar so that the valid URL typed by the user is modified to that of the illegitimate Web site. Pharming may also exploit the Domain Name System (DNS) by causing it to transform the legitimate host name into the invalid site's IP address; this form of pharming is also known as **DNS cache poisoning**.

16. Timing Attack

A **timing attack** explores the contents of a Web browser's cache and stores a malicious cookie on the client's system. The cookie (which is a small quantity of data stored by the Web browser on the local system, at the direction of the Web server) can allow the designer to collect information on how to access password-protected sites. Another attack by the same name involves the interception of cryptographic elements to determine keys and encryption algorithms.

Secure Software Development

Systems consist of hardware, software, networks, data, procedures, and people using the system. Many of the information security issues described in this chapter have their root cause in the software elements of the system. Secure systems require secure, or at least securable, software. The development of systems and the software they use is often accomplished using a methodology, such as the systems development life cycle (SDLC). Many organizations recognize the need to include planning for security objectives in the SDLC they use to create systems, and have put in place procedures to create software that is more able to be deployed in a secure fashion. This approach to software development is known as software assurance, or SA.

Software Assurance and the SA Common Body of Knowledge

The U.S. Department of Defense (DoD) launched a Software Assurance Initiative in 2003. This initial process was led by **Joe Jarzombek** and was endorsed and supported by the Department of Homeland Security (DHS), which joined the program in 2004. This program initiative resulted in the publication of the Secure Software Assurance (SwA) Common Body of Knowledge (CBK).47 A working group drawn from industry, government, and academia was formed to examine two key questions:

1. What are the engineering activities or aspects of activities that are relevant to achieving secure software?
2. What knowledge is needed to perform these activities or aspects?

Based on the findings of this working group, and a host of existing external documents and standards, the SwA CBK was developed and published to serve as a guideline. While this work has not yet been adopted

as a standard or even a policy requirement of government agencies, it serves as a strongly recommended guide to developing more secure applications.

The SwA CBK, which is a work in progress, contains the following sections:

- Nature of Dangers
- Fundamental Concepts and Principles
- Ethics, Law, and Governance
- Secure Software Requirements
- Secure Software Design
- Secure Software Construction
- Secure Software Verification, Validation, and Evaluation
- Secure Software Tools and Methods
- Secure Software Processes
- Secure Software Project Management
- Acquisition of Secure Software
- Secure Software Sustainment

The following sections provides insight into the stages that should be incorporated into the software SDLC.

Software Design Principles

- Economy of mechanism: Keep the design as simple and small as possible.
- Fail-safe defaults: Base access decisions on permission rather than exclusion.
- Complete mediation: Every access to every object must be checked for authority.
- Open design: The design should not be secret, but rather depend on the possession of keys or passwords.
- Separation of privilege: Where feasible, a protection mechanism should require two keys to unlock, rather than one.
- Least privilege: Every program and every user of the system should operate using the least set of privileges necessary to complete the job.
- Least common mechanism: Minimize mechanisms (or shared variables) common to more than one user and depended on by all users.
- Psychological acceptability: It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.

Software Development Security Problems

Some software development problems that result in software that is difficult or impossible to deploy in a secure fashion have been identified as "deadly sins in software security." These twenty problem areas in software development (which is also called software engineering) were originally categorized by John Viega, upon request of Amit Youran, who at the time was the Director of the Department of Homeland Security's National Cyber Security Division. These problem areas are the following:

1. **Buffer Overruns** - Buffers are used to manage mismatches in the processing rates between two entities involved in a communication process. A buffer overrun (or buffer overflow) is an application error that occurs when more data is sent to a program buffer than it is designed to handle. During a buffer overrun, an attacker can make the target system execute instructions, or the attacker can take advantage of some other unintended consequence of the failure. Sometimes this is limited to a denial-of-service attack. In any case, data on the attacked system loses integrity.

2. **Command Injection** - Command injection problems occur when user input is passed directly to a compiler or interpreter. The underlying issue is the developer's failure to ensure that command input is validated before it is used in the program.

3. **Cross-site Scripting** - Cross site scripting (or XSS) occurs when an application running on a Web server gathers data from a user in order to steal it. An attacker can use weaknesses in the Web server environment to insert commands into a user's browser session, so that users ostensibly connected to a friendly Web server are, in fact, sending information to a hostile server. This allows the attacker to acquire valuable information, such as account credentials, account numbers, or other critical data. Often an attacker encodes a malicious link and places it in the target server, making it look less suspicious. After the data is collected by the hostile application, it sends what appears to be a valid response from the intended server.

4. **Failure to Handle Errors** - What happens when a system or application encounters a scenario that it is not prepared to handle? Does it attempt to complete the operation (reading or writing data or performing calculations)? Does it issue a cryptic message that only a programmer could understand? Or does it simply stop functioning? Failure to handle errors can cause a variety of unexpected system behaviors. Programmers are expected to anticipate problems and prepare their application code to handle them.

5. **Failure to Protect Network Traffic** - Traffic on a wired network is also vulnerable to interception in some situations. On networks using hubs instead of switches, any user can install a packet sniffer and collect communications to and from users on that network. Periodic scans for unauthorized packet sniffers, unauthorized connections to the network, and general awareness of the threat can mitigate this problem.

6. **Failure to Store and Protect Data Securely** - Storing and protecting data securely is a large enough issue to be the core subject of this entire text. Programmers are responsible for integrating access controls into, and keeping secret information out of, programs. Access controls, the subject of later chapters, regulate who, what, when, where, and how individuals and systems interact with data. Failure to properly implement sufficiently strong access controls makes the data vulnerable. Overly strict access controls hinder business users in the performance of their duties, and as a result the controls may be administratively removed or bypassed.

7. **Failure to Use Cryptographically Strong Random Numbers** - Most modern cryptosystems, like many other computer systems, use random number generators. However, a decision support system using random and pseudo-random numbers for Monte Carlo method forecasting does not require the same degree of rigor and the same need for true randomness as a system that seeks to implement cryptographic procedures. These "random" number generators use a mathematical algorithm, based on a seed value and another other system component (such as the computer clock) to simulate a random number. Those who understand the workings of such a "random" number generator can predict particular values at particular times.

8. **Format String Problems** - Computer languages often are equipped with built-in capabilities to reformat data while they're outputting it. The formatting instructions are usually written as a "format string." Unfortunately, some programmers may use data from untrusted sources as a format string. An attacker may embed characters that are meaningful as formatting directives (e.g., %x, %d, %p, etc.) into malicious input; if this input is then interpreted by the program as formatting directives (such as an argument to the C printf function), the attacker may be able to access information or overwrite very targeted portions of the program's stack with data of the attacker's choosing.

9. **Neglecting Change Control** - Developers use a process known as change control to ensure that the working system delivered to users represents the intent of the developers. Early in the development process, change control ensures that developers do not work at cross purposes by altering the same programs or parts of programs at the same time. Once the system is in production, change control processes ensure that only authorized changes are introduced and that all changes are adequately tested before being released.

10. **Improper File Access** - If an attacker changes the expected location of a file by intercepting and modifying a program code call, the attacker can force a program to use files other than the ones the program is supposed to use. This type of attack could be used to either substitute a bogus file for a legitimate file (as in password files), or trick the system into running a malware executable. The potential for damage or disclosure is great, so it is critical to protect not only the location of the files but also the method and communications channels by which these files are accessed.

11. **Improper Use of SSL** - If an attacker changes the expected location of a file by intercepting and modifying a program code call, the attacker can force a program to use files other than the ones the program is supposed to use. This type of attack could be used to either substitute a bogus file for a legitimate file (as in password files), or trick the system into running a malware executable. The potential for damage or disclosure is great, so it is critical to protect not only the location of the files but also the method and communications channels by which these files are accessed.

12. **Information Leakage** - One of the most common methods of obtaining inside and classified information is directly or indirectly from an individual, usually an employee.

13. **Integer Bugs (Overflows/Underflows)** - Integer bugs fall into four broad classes: overflows, underflows, truncations, and signedness errors. Integer bugs are usually exploited indirectly—that is, triggering an integer bug enables an attacker to corrupt other areas of memory, gaining control of an application. The memory allocated for a value could be exceeded, if that value is greater than expected, with the extra bits written into other locations. The system may then experience unexpected consequences, which could be miscalculations, errors, crashing or other problems. Even though integer bugs are often used to build a buffer overflow or other memory corruption attack, integer bugs are not just a special case of memory corruption bugs.

14. **Race Conditions** - A race condition is a failure of a program that occurs when an unexpected ordering of events in the execution of the program results in a conflict over access to the same system resource.

    A race condition occurs, for example, when a program creates a temporary file, and an attacker is able to replace it between the time it is created and the time it is used. A race condition can also occur when information is stored in multiple memory threads if one thread stores information in the wrong memory location, by accident or intent.

15. **SQL Injection** - SQL injection occurs when developers fail to properly validate user input before using it to query a relational database.

16. **Use of Weak Password-Based Systems** - Failure to require sufficient password strength, and to control incorrect password entry, is a serious security issue. Password policy can specify the

number and type of characters, the frequency of mandatory changes, and even the reusability of old passwords. Similarly, a system administrator can regulate the permitted number of incorrect password entries that are submitted and further improve the level of protection. Systems that do not validate passwords, or store passwords in easy-to-access locations, are ripe for attack.

17. **Poor Usability** - Employees prefer doing things the easy way. When faced with an "official way" of performing a task and an "unofficial way"—which is easier—they prefer the easier method. The only way to address this issue is to only provide one way—the secure way! Integrating security and usability, adding training and awareness, and ensuring solid controls all contribute to the security of information. Allowing users to default to easier, more usable solutions will inevitably lead to loss.

Assessment

1. Why is information security a management problem? What can management do that technology cannot?
2. Why is data the most important asset an organization possesses? What other assets in the organization require protection?
3. Why do employees constitute one of the greatest threats to information security?
4. What measures can individuals take to protect against shoulder surfing?
5. What are the various types of malware? How do worms differ from viruses? Do Trojan horses carry viruses or worms?
6. How does technological obsolescence constitute a threat to information security? How can an organization protect against it?
7. Does the intellectual property owned by an organization usually have value? If so, how can attackers threaten that value?
8. What are the types of password attacks? What can a systems administrator do to protect against them?
9. What is the difference between a denial-of-service attack and a distributed denial-of-service attack? Which is more dangerous? Why?
10. What methods does a social engineering hacker use to gain information about a user's login ID and password? How would this method differ if it were targeted towards an administrator's assistant versus a data-entry clerk?

References

1. Whitman, Michael, Principles of Information Security, 6th Ed., 2018
2. Compromises to IP, Deviations in QoS, & Espionage or Trespass (Lecture 1.2.1) - Threats to Cybersecurity (Module 1.2) | Coursera. (2019). Coursera. https://www.coursera.org/lecture/foundations-cybersecurity/compromises-to-ip-deviations-in-qos-espionage-or-trespass-lecture-1-2-1-ryoTB
3. What is a computer worm and how does it work? (2019). Norton.com. https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html
4. What Is A Computer Virus? (2020). Norton.com. https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html
5. TechTarget Contributors. (2017). virus hoax. SearchSecurity; TechTarget. https://searchsecurity.techtarget.com/definition/virus-hoax
6. Kaspersky. (2019, February 15). What is a Trojan Virus? Www.Kaspersky.com. https://www.kaspersky.com/resource-center/threats/trojans