



COURSE MANUAL

INFORMATION ASSURANCE AND SECURITY

This course provides students with the theoretical knowledge and practical skills in the implementation of Information Assurance and Security providing relevant solutions for security hardening and information protection through computer vulnerability assessment, secure coding, and computer security hardening techniques.



INFORMATION
TECHNOLOGY

Security and System Administration
Cluster

MODULE 1

INTRODUCTION TO INFORMATION SECURITY

Table of Contents

Lesson Topics

01

Introduction to Information Security

Information security (InfoSec) is the practice of protecting information from unauthorized access, use, disclosure, alteration, or disruption by implementing tools, processes, and methodologies.

02

The Need for Information Security

Information security is essential to protect data from unauthorized access, ensuring confidentiality, integrity, and availability, and preventing financial and reputational damage.

03

Threat and Attacks

A threat is a potential or intentional action that could harm a system or asset, while an attack is the actual malicious act that exploits a vulnerability to cause damage.

04

Laboratory Activity

This laboratory activity focuses on web application development, involving the design, creation, testing, and deployment of interactive web-based systems.

Introduction to Information Security



Learning Outcomes:

- Identify key terms in Information Security.
- Identify the components of an Information System
- Describe Information Security as an Art or Science.



Understanding Principles of Information Security

James Anderson, executive consultant at Emagined Security, Inc., believes information security in an enterprise is a “well-informed sense of assurance that the information risks and controls are in balance.” He is not alone in his perspective. Many information security practitioners recognize that aligning information security needs with business objectives must be the top priority.

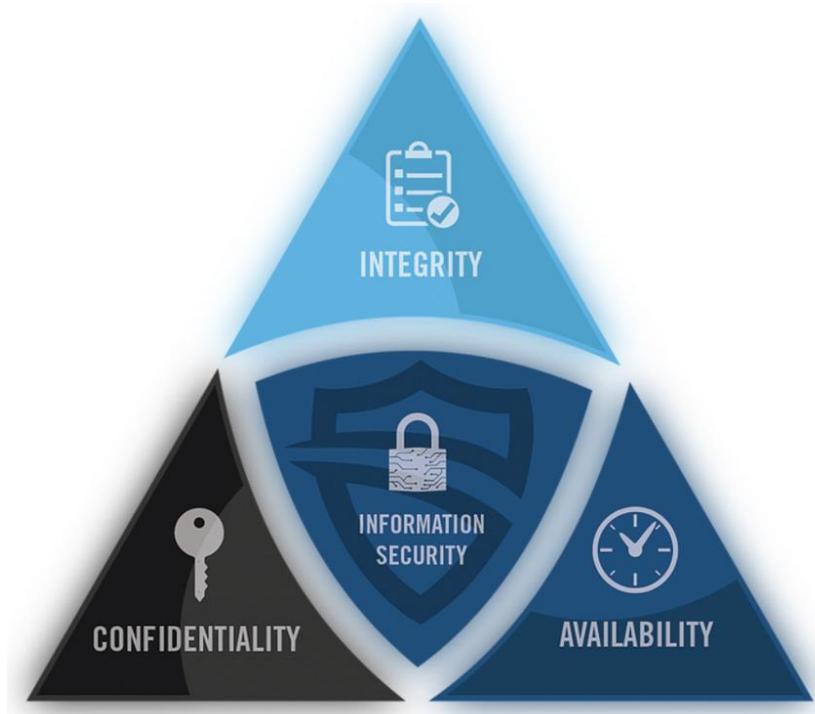
What Is Security?

Computer security in the early days of computers, this term specified the need to secure the physical location of computer technology from outside threats. This term later came to represent all actions taken to preserve computer systems from losses. It has evolved into the current concept of information security as the scope of protecting information in an organization has expanded. In general, **security** is “the quality or state of being secure--to be free from danger.” It means to be protected from adversaries--from those who would do harm, intentionally or otherwise. A successful organization should have the following multiple layers of security in place for the protection of its operations:

- **Physical Security** – To protect the physical items, objects, or areas of an organization from unauthorized access and misuse.
- **Personal 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 an organization’s communications media, technology, and content.
- **Network Security** – To protect networking components, connections, and contents.

Security is the protection of information and its critical elements, including systems and hardware that use, store, and transmit that information. Necessary tools in security implementation are policy, awareness, training, education, technology

C.I.A. triangle is the industry standard for computer security since the development of the mainframe. The standard is based on three characteristics that describe the utility of information: confidentiality, integrity, and availability.



Critical Characteristics of Information

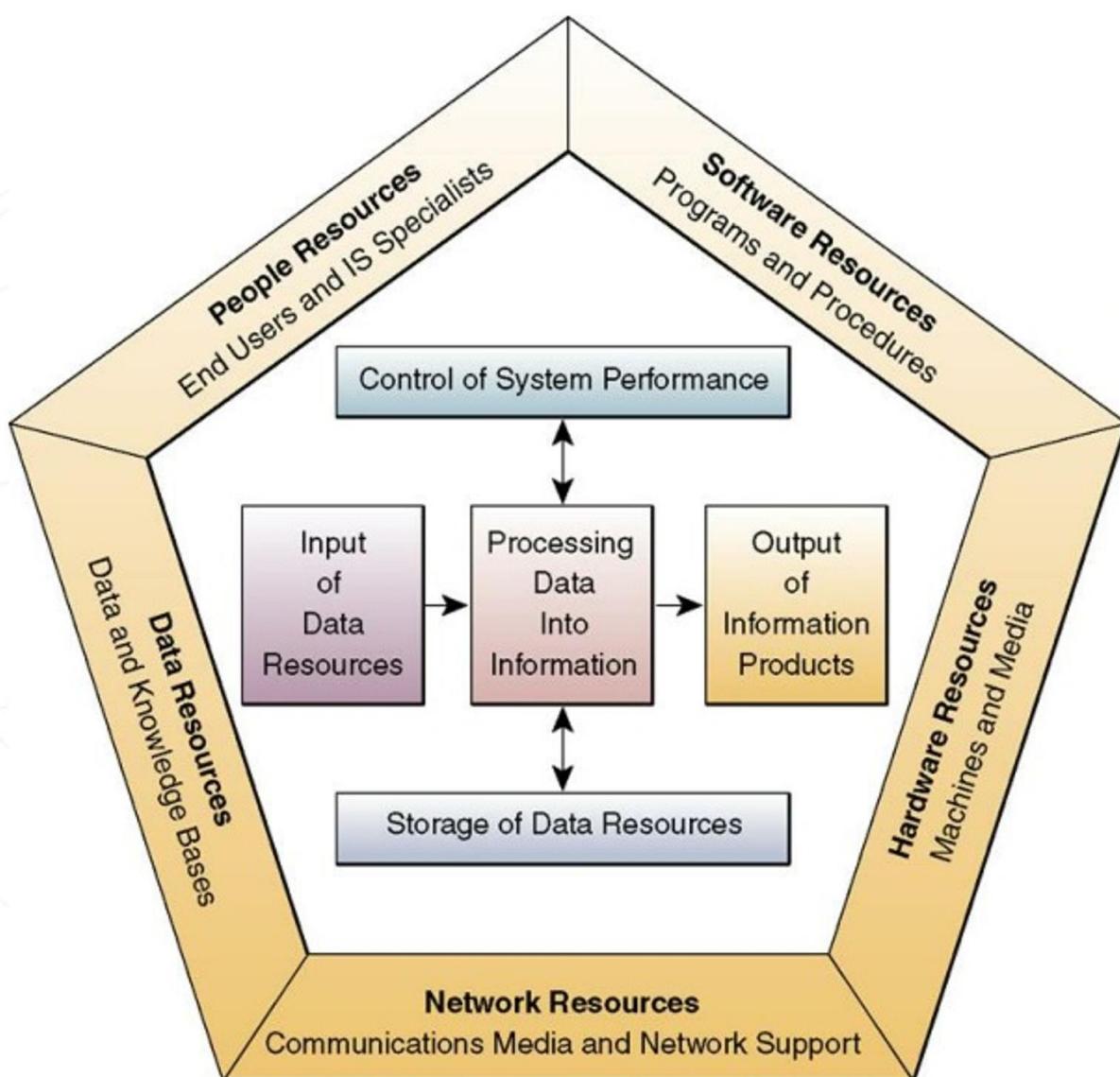
The value of information comes from the characteristics it possesses. When a characteristic of information changes, the value of that information either increases or, more commonly, decreases. Some characteristics affect information's value to users more than others, depending on circumstances. Each critical characteristic of information—that is, the expanded C.I.A. triangle—is defined in the following sections.

- **Availability** – Enables users who need to access information to do so without interference or obstruction and in the required format. The information is said to be available to an authorized user when and where needed and in the correct format.
- **Accuracy** – Free from mistake or error and having the value that the end user expects. If information contains a value different from the user's expectations due to the intentional or unintentional modification of its content, it is no longer accurate.

- **Authenticity** – The quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is the information that was originally created, placed, stored, or transferred.
- **Confidentiality** – The quality or state of preventing disclosure or exposure to unauthorized individuals or systems.
- **Integrity** – The quality or state of being 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.
- **Utility** – The quality or state of having value for some purpose or end. Information has value when it serves a particular purpose. This means that if information is available, but not in a format meaningful to the end user, it is not useful.
- **Possession** – The quality or state of having ownership or control of some object or item. Information is said to be in possession if one obtains it, independent of format or other characteristic. 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.

Understanding the Components of an Information System

Information system (IS) is entire set of software, hardware, data, people, procedures, and networks necessary to use information as a resource in the organization. The six critical components of hardware, software, networks, people, procedures, and data enable information to be input, processed, output, and stored.



Components of an Information System

To fully understand the importance of information security, it is necessary to briefly review the elements of an information system. Each of these IS components has its own strengths and weaknesses, as well as its own characteristics and uses. Each component of the information system also has its own security requirements.

Software

The software component of an IS includes 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. The information technology industry is rife with reports warning of holes, bugs, weaknesses, or other fundamental problems in software. In fact, many facets of daily life are affected by buggy software, from smartphones that crash to flawed automotive control computers that lead to recalls. Software carries the lifeblood of information through an organization. Unfortunately, software programs are often created under the constraints of project management, which limit time, costs, and manpower. Information security is all too often implemented as an afterthought rather than developed as an integral component from the beginning. In this way, software programs become an easy target of accidental or intentional attacks.

Hardware

Hardware is the physical technology that houses and executes the software, stores and transports the data, and provides interfaces for the entry and removal of information from the system. Physical security policies deal with hardware as a physical asset and with the protection of physical assets from harm or theft. Applying the traditional tools of physical security, such as locks and keys, restricts access to and interaction with the hardware components of an information system. Securing the physical location of computers and the computers themselves is important because a breach of physical security can result in a loss of information. Unfortunately, most information systems are built on hardware platforms that cannot guarantee any level of information security if unrestricted hardware access is possible.

People

Though often overlooked in computer security considerations, people have always been a threat to information security.

Data

Data stored, processed, and transmitted by a computer system must be protected. Data is often the most valuable asset of an organization and therefore is the main target of intentional attacks. Systems developed in recent years are likely to make use of database management systems. When used properly, they should improve the security of the data and the applications that rely on the data. Unfortunately, many system development projects do not make full use of the database management system's security capabilities, and in some cases the database is implemented in ways that make them less secure than traditional file systems. Because data and information exist in physical form in many organizations as paper reports, handwritten notes, and computer printouts, the protection of physical information is as important as the protection of electronic, computer-based information.

Procedures

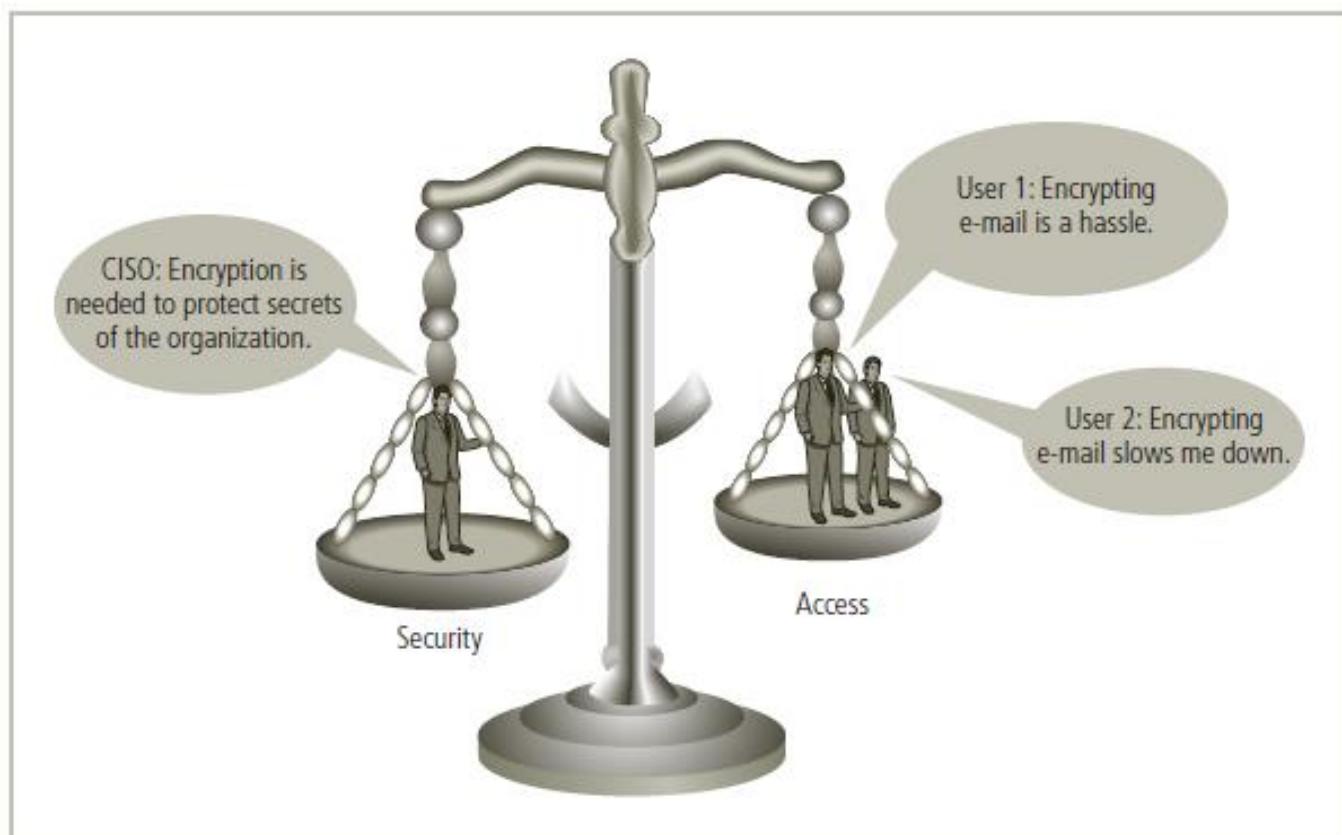
Procedures are another frequently overlooked component of an IS. Procedures are written instructions for accomplishing a specific task. Most organizations distribute procedures to employees so they can access the information system, but many of these companies often fail to provide proper education for using the procedures safely. Educating employees about safeguarding procedures is as important as physically securing the information system. After all, procedures are information in their own right. Therefore, knowledge of procedures, as with all critical information, should be disseminated among members of an organization on a need-to-know basis.

Network

Networking is the IS 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. The physical technology that enables network functions is becoming more accessible to organizations of every size. Applying the traditional tools of physical security, such as locks and keys, to restrict access to the system's hardware components is still important. However, when computer systems are networked, this approach is no longer enough. Steps to provide network security are essential, as is implementing alarm and intrusion systems to make system owners aware of ongoing compromises.

Balancing Information Security and Access

To achieve balance—that is, to operate an information system that satisfies the user and the security professional—the security level must allow reasonable access, yet protect against threats. Figure shows some of the competing voices that must be considered when balancing information security and access.



Because of today's security concerns and issues, an information system or data processing department can get too entrenched in the management and protection of systems. An imbalance can occur when the needs of the end user are undermined by obsessive focus on protecting and administering the information systems. Information security technologists and end users must recognize that both groups share the same overall goals of the organization—to ensure that data is available when, where, and how it is needed, with minimal delays or obstacles. In an ideal world, this level of availability can be met even after addressing concerns about loss, damage, interception, or destruction.

Approaches to Information Security Implementation

The implementation of information security in an organization must begin somewhere and cannot happen overnight. Securing information assets is an incremental process that requires coordination, time, and patience. Information security can begin as a grassroots effort in which systems administrators attempt to improve the security of their systems. This is often referred to as a bottom-up approach. The key advantage of the bottom-up approach is the technical expertise of individual administrators. By working with information systems on a day-to-day basis, these administrators possess in-depth knowledge that can greatly enhance the development of an information security system. They know and understand the threats to their systems and the mechanisms needed to protect them successfully. Unfortunately, the bottom-up approach seldom works because it lacks critical features such as participant support and organizational staying power. The top-down approach has a higher probability of success. With this approach, the project is initiated by upper-level managers who issue policies, procedures, and processes; dictate the goals and expected outcomes; and determine accountability for each required action. This approach has strong upper management support, a dedicated champion, usually dedicated funding, a clear planning and implementation process, and the means of influencing organizational culture. The most successful kind of top-down approach also involves a formal development strategy known as a systems development life cycle.

Understanding Information Security Paradigm

Information Security: Is It an Art or a Science?

Given the level of complexity in today's information systems, the implementation of information security has often been described as a combination of art and science. System technologists, especially those with a gift for managing and operating computers and computer-based systems, have long been suspected of using more than a little magic to keep the systems running as expected. In information security, such technologists are sometimes called security artisans. Everyone who has studied computer systems can appreciate the anxiety most people feel when faced with complex technology.

Security as Art

The administrators and technicians who implement security can be compared to a painter applying oils to canvas. A touch of color here, a brush stroke there, just enough to represent the image the artist wants to convey without overwhelming the viewer—or in security terms, without overly restricting user access. There are no hard and fast rules regulating the installation of various security mechanisms, nor are there many universally accepted complete solutions. While many manuals exist to support individual systems, no manual can help implement security throughout an entire interconnected system. This is especially true given the complex levels of interaction among users, policy, and technology controls.

Security as Science

Technology developed by computer scientists and engineers—which is designed for rigorous performance levels—makes information security a science as well as an art. Most scientists agree that specific conditions cause virtually all actions in computer systems. Almost every fault, security hole, and systems malfunction is a result of the interaction of specific hardware and software. If the developers had sufficient time, they could resolve and eliminate these faults. The faults that remain are usually the result of technology malfunctioning for any of a thousand reasons. There are many sources of recognized and approved security methods and techniques that provide sound technical security advice. Best practices, standards of due care, and other tried-and-true methods can minimize the level of guesswork necessary to secure an organization's information and systems.

Security as a Social Science

A third view to consider is information security as a social science, which integrates components of art and science and adds another dimension to the discussion. Social science examines the behavior of people as they interact with systems, whether they are societal systems or, as in this context, information systems. Information security begins and ends with the people inside the organization and the people who interact with the system, intentionally or otherwise. End users who need the very information that security personnel are trying to protect may be the weakest link in the security chain. By understanding some behavioral aspects of organizational science and change management, security administrators can greatly reduce the levels of risk caused by end users and create more acceptable and supportable security profiles. These measures, coupled with appropriate policy and training issues, can substantially improve the performance of end users and result in a more secure information system.

The Need for Information Security



Learning Outcomes:

- Describe the need for Information Security in an organization.



Understanding Business Need for Security

Unlike any other business or information technology program, the primary mission of an information security program is to ensure that information assets—information and the systems that house them—remain safe and useful. Organizations expend a lot of money and thousands of man-hours to maintain their information assets. If threats to these assets didn't exist, those resources could be used exclusively to improve the systems that contain, use, and transmit the information. However, the threat of attacks on information assets is a constant concern, and the need for information security grows along with the sophistication of the attacks. Organizations must understand the environment in which information assets reside so their information security programs can address actual and potential problems.

Key Terms

- **data** Items of fact collected by an organization. Data includes raw numbers, facts, and words. Student quiz scores are a simple example of data.
- **Information** Data that has been organized, structured, and presented to provide additional insight into its context, worth, and usefulness. For example, a student's class average can be presented in the context of its value, as in "90 ¼ A."
- **Information asset** The focus of information security; information that has value to the organization, and the systems that store, process, and transmit the information.

Business Needs First

Key Terms

- **data security** Commonly used as a surrogate for information security, data security is the focus of protecting data or information in its various states—at rest (in storage), in processing, and in transmission (over networks).

Information security performs four important functions for an organization:

- Protecting the organization's ability to function
- Protecting the data and information the organization collects and uses
- Enabling the safe operation of applications running on the organization's IT systems
- Safeguarding the organization's technology assets

Protecting Functionality

General management, IT management, and information security management are each responsible for facilitating the information security program that protects the organization's ability to function. Although many business and government managers shy away from addressing information security because they perceive it to be a technically complex task, implementing information security actually has more to do with management than technology.

Protecting Data that Organizations Collect and Use

Many organizations realize that one of their most valuable assets is their data, because without data, an organization loses its record of transactions and/or its ability to deliver value to its customers. Protecting data in motion and data at rest are both critical aspects of information security. An effective information security program is essential to the protection of the integrity and value of the organization's data.

Enabling the Safe Operation of Applications

Today's organizations are under immense pressure to create and operate integrated, efficient, and capable applications. The modern organization needs to create an environment that safeguards applications using the organization's IT systems, particularly the environment of the organization's infrastructure. Once the infrastructure is in place, management must understand it has not abdicated to the IT department its responsibility to make choices and enforce decisions, but must continue to oversee the infrastructure.

Safeguarding the Technology Assets in Organizations

To perform effectively, organizations must add secure infrastructure services based on the size and scope of the enterprise. When an organization grows and more capabilities are needed, additional security services may have to be provided locally. Likewise, as the organization's network grows to accommodate changing needs, more robust technology solutions may be needed to replace security programs the organization has outgrown.

Threats and Attacks



Learning Outcomes:

- Identify the different threats and attacks posed to Information Systems.



Understanding Cybercrime

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.



Cybercrime is committed by cybercriminals or hackers



Most cybercrimes are carried out in order to generate profit



Cybercrimes are carried out against computers or devices to directly damage, spread malware, steal information, etc.

Types of Cybercriminals

Understanding the types of cyber criminals and their techniques can help protect your organization from a data breach.



Social Engineer

Cybercriminals pretending to be someone else can trick unsuspecting employees to compromise data.



Hacker

Cybercriminals that often hack computers for no criminal reason.



Rogue Employee

Disgruntled employees present an insider threat to data considered to be the highest risk in organizations.



Spear Phisher

Cybercriminals pretending to be a legitimate email sender to compromise data.



Ransom Artist

Cybercriminals that exert pressure on the victim to pay them a sum of money to regain access to data.

Understanding Threats and Attacks to Information Security

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. To make sound decisions about information security, management must be informed about the various threats to an organization's people, applications, data, and information systems. A **threat** represents a potential risk to an information asset, whereas an **attack** represents an ongoing act against the asset that could result in a loss. **Threat agents** damage or steal an organization's information or physical assets by using exploits to take advantage of vulnerabilities where controls are not present or no longer effective. Unlike threats, which are always present, attacks exist only when a specific act may cause a loss. A vulnerability is a potential weakness in an asset or its defensive control system(s). For example, the threat of damage from a thunderstorm is present throughout the summer in many places, but an attack and its associated risk of loss exist only for the duration of an actual thunderstorm. The following sections discuss each of the major types of threats and corresponding attacks facing modern information assets.



Threats to Information Security

Category of threat	Attack examples
Compromises to intellectual property	Piracy, copyright infringement
Deviations in quality of service	Internet service provider (ISP), power, or WAN service problems
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, floods, earthquakes, lightning
Human error or failure	Accidents, employee mistakes
Information extortion	Blackmail, information disclosure
Sabotage or vandalism	Destruction of systems or information
Software attacks	Viruses, worms, macros, denial of service
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

The 12 Categories of Threats to Information Security⁷

© Cengage Learning 2015

Compromises to Intellectual Property

Many organizations create or support the development of intellectual property as part of their business operations. **Intellectual property** is defined as “the ownership of ideas and control over the tangible or virtual representation of those ideas.” Intellectual property for an organization includes trade secrets, copyrights, trademarks, and patents. Once intellectual property (IP) has been defined and properly identified, breaches to IP constitute a threat to the security of this information. Most common IP breaches involve the unlawful use or duplication of software-based intellectual property, known as **software piracy**. In addition to the laws surrounding software piracy, two watchdog organizations investigate allegations of software abuse: Software & Information Industry Association (SIIA), formerly the Software Publishers Association, and the Business Software Alliance (BSA). Enforcement of copyright violations, piracy, and the like has been attempted through a number of technical security mechanisms, including digital watermarks, embedded code, copyright codes, and even the intentional placement of bad sectors on software media that have been used to enforce copyright laws. The most common tool is a unique software registration code in combination with an end-user license agreement (EULA) that usually pops up during the installation of new software, requiring users to indicate that they have read and agree to conditions of the software’s use.

Deviations in Quality of Service

An organization's information system depends on the successful operation of many interdependent support systems, including power grids, data and telecommunications networks, parts suppliers, service vendors, and even janitorial staff and garbage haulers. Any of these support systems can be interrupted by severe weather, employee illnesses, or other unforeseen events. Deviations in quality of service can result from such accidents as a backhoe taking out an ISP's fiber-optic link. The backup provider may be online and in service, but may be able to supply only a fraction of the bandwidth the organization needs for full service. This degradation of service is a form of **availability disruption**. Irregularities in Internet service, communications, and power supplies can dramatically affect the availability of information and systems.

Internet Service Issues

For organizations that rely heavily on the Internet and the Web to support continued operations, the threat of the potential loss of Internet service can lead to considerable loss in the availability of information. Many organizations have sales staff and telecommuters working at remote locations. When an organization places its Web servers in the care of a Web hosting provider, that outsourcer assumes responsibility for all Internet services as well as for the hardware and operating system software used to operate the Web site. These Web hosting services are usually arranged with a service level agreement (SLA). When a service provider fails to meet the terms of the SLA, the provider may accrue fines to cover losses incurred by the client, but these payments seldom cover the losses generated by the outage.

Communications and Other Service Provider Issues

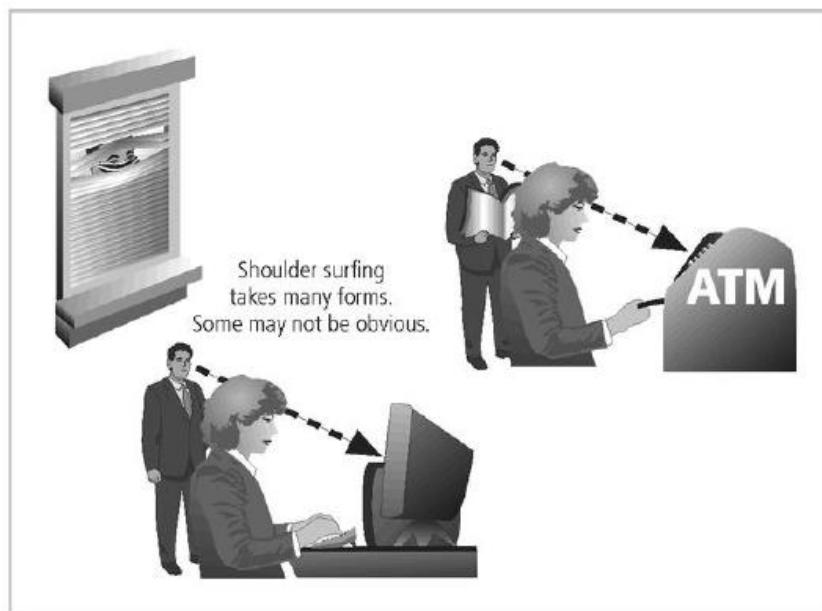
Other utility services can impact organizations as well. Among these are telephone, water, wastewater, trash pickup, cable television, natural or propane gas, and custodial services. The threat of loss of these services can lead to the inability of an organization to function properly.

Power Irregularities

The threat of irregularities from power utilities is common and can lead to fluctuations such as power excesses, power shortages, and power losses. Since sensitive electronic equipment, especially networking equipment, computers, and computer-based systems are susceptible to fluctuations, controls can be applied to manage power quality.

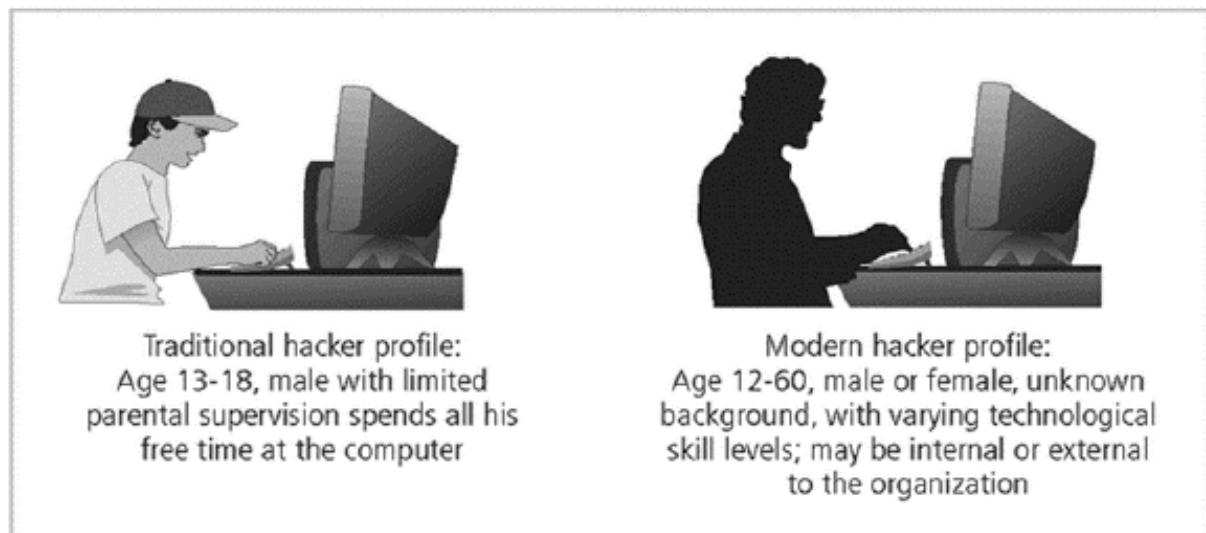
Espionage or Trespass

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 person gains access to information an organization is trying to protect, the act 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 legal—for example, using a Web browser to perform market research. These legal techniques are collectively called **competitive intelligence**. When information gatherers employ techniques that cross a legal or ethical threshold, they are conducting **industrial espionage**. Some forms of espionage are relatively low tech. is called shoulder surfing. This technique is used in public or semipublic settings when people gather information they are not authorized to have. Instances of **shoulder surfing** occur at computer terminals, desks, and ATMs; on a bus, airplane, or subway, where people use smartphones and tablet PCs; and in other places where employees may access confidential information.



Acts of **trespass** can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems without permission. 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. These control methods and technologies employ multiple layers or factors to protect against unauthorized access and trespass. The classic perpetrator of espionage or trespass is the hacker, who is frequently glamorized in fictional accounts as a person who stealthily manipulates a maze of computer networks, systems, and data to find information that solves the mystery and heroically saves the day.

Hacker Skills and Abilities Hackers possess a wide range of skill levels, as with most technology users. However, most hackers are grouped into two general categories: the expert hacker and the novice hacker.



The first is the expert hacker, who develops software scripts and codes exploits used by the second category, the novice, or unskilled hacker. The **expert hacker** is usually a master of several programming languages, networking protocols, and operating systems and also exhibits a mastery of the technical environment of the chosen targeted system. However, expert hackers have now become bored with directly attacking systems and have turned to writing software. The software they are writing are automated exploits that allow **novice hackers** to become script kiddies, hackers of limited skill who use expert-written software to exploit a system but do not fully understand or appreciate the systems they hack. As a result of preparation and continued vigilance, attacks conducted by scripts are usually predictable and can be adequately defended against. A new category of hacker has emerged over the last few years. The **professional hacker** seeks to conduct attacks for personal benefit or the benefit of an employer, which is typically a crime organization or illegal government operation. The professional hacker should not be confused with the penetration tester, who has authorization from an organization to test its information systems and network defense and is expected to provide detailed reports of the findings. The primary differences between professional hackers and penetration testers are the authorization provided and the ethical professionalism displayed. Penetration tester is an information security professional with authorization to attempt to gain system access in an effort to identify and recommend resolutions for vulnerabilities in those systems.

There are other terms for system rule breakers:

- The term **cracker** is now commonly associated with an individual who “cracks” or removes the software protection from an application designed to prevent unauthorized duplication.
- A **phreaker** hacks the public telephone network to make free calls, disrupt services, and generally wreak havoc.

Forces of Nature

Forces of nature, sometimes called acts of God, can present some of the most dangerous threats because they usually occur with 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 people's lives but the storage, transmission, and use of information. Because it is not possible to avoid threats from forces of nature, organizations must implement controls to limit damage and prepare contingency plans for continued operations, such as disaster recovery plans, business continuity plans, and incident response plans. Another term you may encounter, force majeure, can be translated as “superior force,” which includes forces of nature as well as civil disorder and acts of war.

Human Error or Failure

This category includes acts performed without intent or malicious purpose or in ignorance by an authorized user. When people use information systems, mistakes happen. Similar errors happen when people fail to follow established policy. Inexperience, improper training, and incorrect assumptions are just a few things that can cause human error or failure. Regardless of the cause, even innocuous mistakes can produce extensive damage.



One of the greatest threats to an organization's information security is its own employees, as they are the threat agents closest to the information. Because employees use data and information 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. Human error or failure often can be prevented with training, ongoing awareness activities, and controls. These controls range from simple activities, such as requiring the user to type a critical command twice, to more complex procedures, such as verifying commands by a second party.

Information Extortion

The threat of information extortion is the possibility of an attacker or formerly trusted insider stealing information from a computer system and demanding compensation for its return or for an agreement to not disclose the information. Extortion is common in credit card number theft.

Sabotage or Vandalism

Equally popular today is the assault on the electronic face of an organization, its Web site. This category of threat addresses the individual or group of individuals who want to deliberately sabotage the operations of a computer system or business or perform acts of vandalism to either destroy an asset or damage the image of the organization. These threats can range from petty vandalism by employees to organized sabotage against an organization. Organizations frequently rely on image to support the generation of revenue, so if an organization's Web site is defaced, a drop in consumer confidence is probable, reducing the organization's sales and net worth. 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 in what are described as hacktivist or cyberactivity operations. A more extreme version is referred to as cyberterrorism.

Software Attacks

Deliberate software attacks occur when an individual or group designs and deploys software to attack a system. This attack can consist of specially crafted software that attackers trick users into installing on their systems. This software can be used to overwhelm the processing capabilities of online systems or to gain access to protected systems by hidden means.

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 manifest themselves periodically, resulting in faults that are not easily repeated. Thus, equipment can sometimes stop working or work in unexpected ways.

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 failures that range from bugs to untested failure conditions. Sometimes these bugs are not errors, but 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 they can cause serious security breaches.

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 losing 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 clear, management must take immediate action. IT professionals play a large role in the identification of probable obsolescence.

Software Attacks

Malware is referred to as malicious code or malicious software. Other attacks that use software, like redirect attacks and denial-of-service attacks, also fall under this threat. These software components or programs are designed to damage, destroy, or deny service to targeted systems. Malicious code attacks include the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information. The most state-of-the-art malicious code attack is the polymorphic worm, or multi-vector worm. These attack programs use up to six known attack vectors to exploit a variety of vulnerabilities in common information system devices. Other forms of malware include covert software applications—bots, spyware, and adware—that are designed to work out of users' sight or be triggered by an apparently innocuous user action. **Bots** are often the technology used to implement Trojan horses, logic bombs, back doors, and spyware. **Spyware** is placed on a computer to secretly gather information about the user and report it.

- **Virus**

A computer virus consists of code segments (programming instructions) that perform malicious actions. This code behaves much like a virus pathogen that attacks animals and plants, using the cell's own replication machinery to propagate the attack beyond the initial target. The code attaches itself to an existing program and takes control of the program's access to the targeted computer. The virus-controlled target program then carries out the virus plan by replicating itself into additional targeted systems. Often, users unwittingly help viruses get into a system.

Viruses can be classified by how they spread themselves. Among the most common types of information system viruses are the **macro virus**, which is embedded in automatically executing macro code used by word processors, spreadsheets, and database applications, and the **boot virus**, which infects the key operating system files in a computer's boot sector.

Alternatively, viruses may be classified as memory-resident viruses or non-memory-resident viruses, depending on whether they persist in a computer system's memory after they have been executed.

Resident viruses are capable of reactivating when the computer is booted and continuing their actions until the system is shut down, only to restart the next time the system is booted.

- **Worms**

A type of malware that is capable of activation and replication without being attached to an existing program. The complex behavior of worms can be initiated with or without the user downloading or executing the file. Once the worm has infected a computer, it can redistribute itself to all e-mail addresses found on the infected system. Furthermore, a worm can deposit copies of itself onto all Web servers that the infected system can reach; users who subsequently visit those sites become infected. Worms also take advantage of open shares found on the network in which an infected system is located. The worms place working copies of their code onto the server so that users of the open shares are likely to become infected.

- **Trojan Horses**

Trojan horses are frequently disguised as helpful, interesting, or necessary pieces of software, such as the readme.exe files often included with shareware or freeware packages. Like their namesake in Greek legend, once Trojan horses are brought into a system, they become activated and can wreak havoc on the unsuspecting user.

- **Polymorphic Threats**

A polymorphic threat actually evolves, changing its size and other external file characteristics to elude detection by antivirus software programs.

- **Virus and Worm Hoaxes**

As frustrating as viruses and worms are, perhaps more time and money are spent resolving virus hoaxes. Well-meaning people can disrupt the harmony and flow of an organization when they send group e-mails warning of supposedly dangerous viruses that don't exist. When people fail to follow virus-reporting procedures in response to a hoax, the network becomes overloaded and users waste time and energy forwarding the warning message to everyone they know, posting the message on bulletin boards, and trying to update their antivirus protection software.

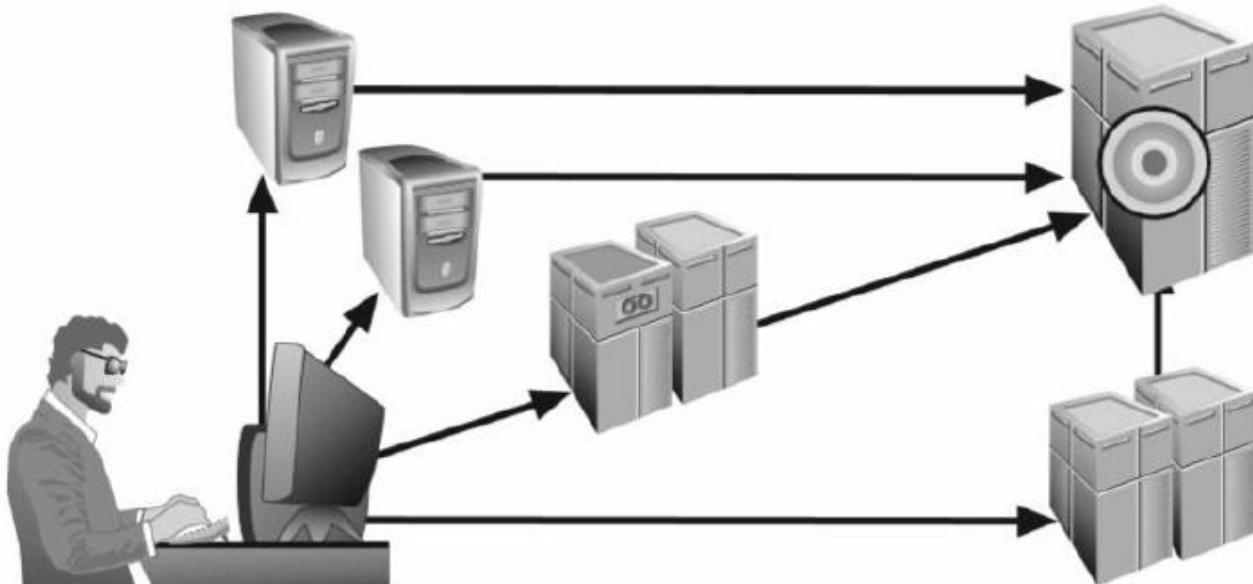
Back Doors

A malware payload that provides access to a system by bypassing normal access controls. A back door is also an intentional access control bypass left by a system designer to facilitate development.

Quality of Service Attacks

In a denial-of-service attack, a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle.

In a distributed denial-of-service attack, dozens or even hundreds of computers (known as zombies) are compromised, loaded with DoS attack software, and then remotely activated by the hacker to conduct a coordinated attack.



© Cengage Learning 2015

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. In a distributed denial-of-service (DDoS) attack, 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 bots or zombies, machines that are directed remotely by the attacker (usually via a transmitted command) to participate in the attack. DDoS attacks are more difficult to defend against, and currently there are no controls that any single organization can apply.

Email Attacks

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. A form of e-mail attack that is also a DoS attack is called a **mail bomb**. It can be accomplished using traditional e-mailing techniques 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 of the attackers' choice. If many such systems are tricked into participating, the target e-mail address is buried under thousands or even millions of unwanted e-mails. Although **phishing attacks** occur via e-mail, they are much more commonly associated with a method of social engineering designed to trick users to perform an action, rather than simply making the user a target of a DoS e-mail attack.

Communications Interception Attacks

Packet Sniffer

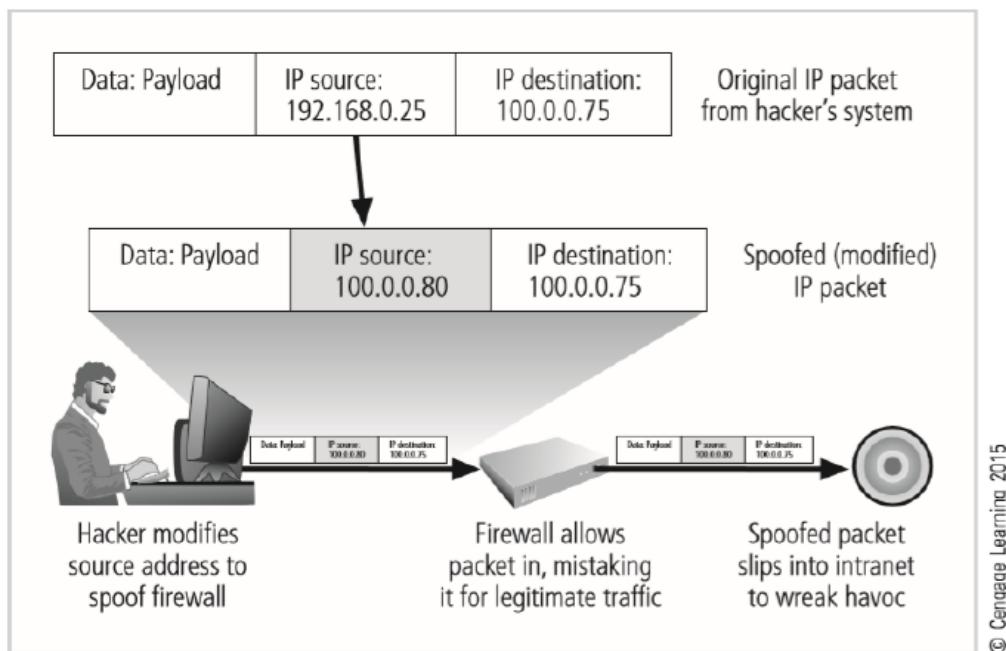
A packet sniffer (or simply sniffer) can monitor data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This feature makes them a favorite weapon in the hacker's arsenal. Sniffers often work on TCP/IP networks. Sniffers add risk to networks 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.

Pharming

Pharming attacks often use Trojans, worms, or other virus technologies to attack an Internet browser's address bar so that the valid URL the user types is modified to be that of an illegitimate Web site. A form of pharming called Domain Name System (DNS) cache poisoning targets the Internet DNS system, corrupting legitimate data tables. The key difference between pharming and the social engineering attack called phishing is that the latter requires the user to actively click a link or button to redirect to the illegitimate site, whereas pharming attacks modify the user's traffic without the user's knowledge or active participation.

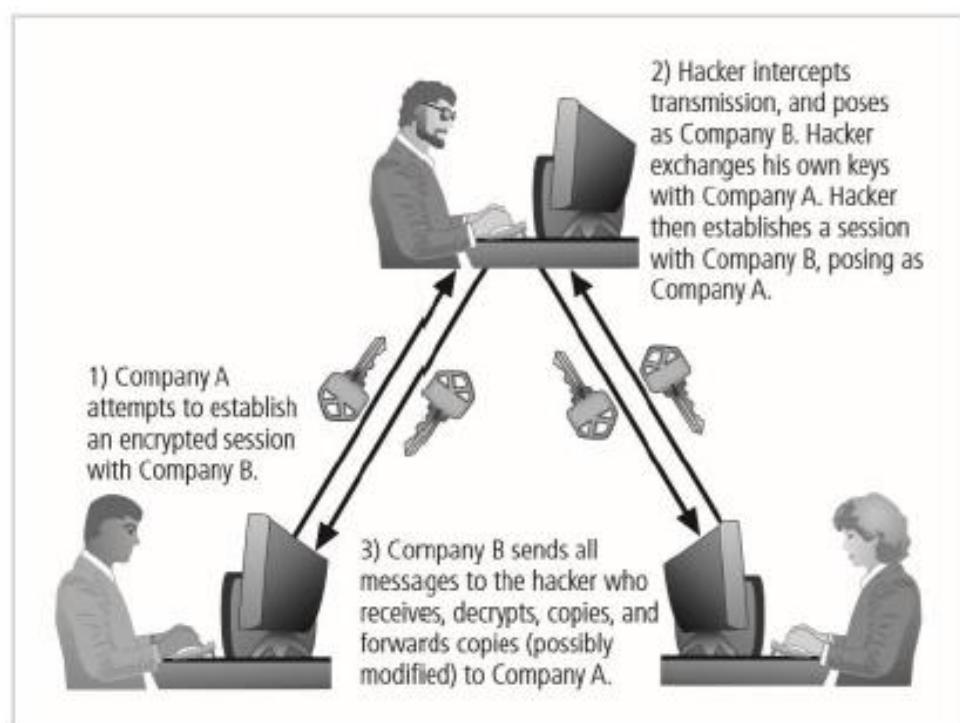
Spoofing

A technique for gaining unauthorized access to computers using a forged or modified source IP address to give the perception that messages are coming from a trusted host.



Man-in-the-Middle

In the well-known man-in-the-middle attack, an attacker monitors (or sniffs) packets from the network, modifies them, and inserts them back into the network. In a TCP hijacking attack, also known as session hijacking, the attacker uses address spoofing to impersonate other legitimate entities 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.



Password Attacks

Password attacks fall under the category of espionage or trespass just as lock-picking falls under breaking and entering. Attempting to guess or reverse-calculate a password is often called cracking. There are a number of alternative approaches to password cracking:

Brute Force

The application of computing and network resources to try every possible password combination is called a brute force password attack. If attackers can narrow the field of target accounts, they can devote more time and resources to these accounts. This is one reason to always change the password of the manufacturer's default administrator account.

Dictionary Attacks

The dictionary password attack, or simply dictionary attack, is a variation of the brute force attack that narrows the field by using a dictionary of common passwords and includes information related to the target user, such as names of relatives or pets, and familiar numbers such as phone numbers, addresses, and even Social Security numbers. Organizations can use similar dictionaries to disallow passwords during the reset process and thus guard against passwords that are easy to guess. In addition, rules requiring numbers and special characters in passwords make the dictionary attack less effective.

Rainbow Tables

A far more sophisticated and potentially much faster password attack is possible if the attacker can gain access to an encrypted password file, such as the Security Account Manager (SAM) data file. While these password files contain hashed representations of users' passwords—not the actual passwords, and thus cannot be used by themselves—the hash values for a wide variety of passwords can be looked up in a database known as a rainbow table.

Social Engineering

While social engineering is discussed in detail later in the section called “Human Error or Failure,” it is worth mentioning here as a mechanism to gain password information. Attackers posing as an organization’s IT professionals may attempt to gain access to systems information by contacting low-level employees and offering to help with their computer issues. After all, what employee doesn’t have issues with computers? By posing as a friendly helpdesk or repair technician, the attacker asks employees for their usernames and passwords, then uses the information to gain access to organizational systems. Some even go so far as to actually resolve the user’s issues. Social engineering is much easier than hacking servers for password files.

Laboratory Activity



Web Application Development

As a developer, your team is tasked to develop a small-medium business enterprise web application (eCommerce, Inventory System, Information System or Thesis/Capstone-related Projects) that will make use of database with some basic CRUD functionalities. Use preferably the ff. web development tools or you may choose the web development framework of your choice.

Web Application Security



In this activity, you will create a basic web application with CRUD (Create, Read, Update, Delete) functionalities. This application will serve as the foundational system for all succeeding activities, including vulnerability testing and secure implementation. The goal is to simulate a real-world scenario where security must be integrated into an existing system.

Show proof of your activity completion by providing clear screenshot of your entire desktop environment based on the tasks performed. Screenshot must be included in the activity template provided in MS Teams Assignment.

LESSON SUMMARY

Information security is a “well-informed sense of assurance that the information risks and controls are in balance”.

Computer security began immediately after first mainframes were developed.

Information system (IS) is entire set of software, hardware, data, people, procedures, and networks necessary to use information as a resource in the organization.

Successful organizations have multiple layers of security in place: physical, personal, operations, communications, network, and information.

Security should be considered a balance between protection and availability.

Information security has been described as both an art and a science, and it comprises many aspects of social science as well.

Unlike any other aspect of IT, information security’s primary mission to ensure things stay the way they are

Information security performs four important functions:

- Protects organization’s ability to function
- Enables safe operation of applications implemented on organization’s IT systems
- Protects data the organization collects and uses
- Safeguards the technology assets in use at the organization

Threats are potential risks to an asset’s value. An attack is a deliberate act that takes advantage of an exploit to compromise a controlled system. An attack is accomplished by a threat agent. A vulnerability is a potential weakness in an asset or its defensive controls.

Management effectively protects its information through policy, education, training, and technology controls

Attack: a deliberate act that exploits vulnerability

Threats or dangers facing an organization’s people, information, and systems fall into the following categories:

- Compromises to intellectual property
- Deviations in quality of service
- Espionage or trespass
- Forces of nature
- Human error or failure
- Information extortion
- Sabotage or vandalism
- Software attacks
- Technical hardware failures or errors
- Technical software failures or errors
- Technological obsolescence
- Theft

KEY TERMS

- Computer Security
- C.I.A. Triangle
- Accuracy
- Authenticity
- Availability
- Confidentiality
- Integrity
- Possession
- Utility
- Information System
- Bottom-up Approach
- Top-down Approach
- Attack
- Exploit
- Threat
- Vulnerability
- Hacker
- Expert Hacker
- Cracker
- Phreaker
- Cracking
- Information Extortion
- Malware
- Virus
- Worm
- Trojan Horse
- Back Door
- Bot
- Denial-of-service (DoS)
- Distributed Denial-of-service (DDoS)
- Mail Bomb
- Spam
- Packet Sniffer
- Man-in-the-middle
- Pharming
- Sniffer
- Spoofing
- Theft

REFERENCES

99

Electronic Books

- Whiteman, et.al. "Principles of Information Security", 3rd Edition