UNIT – II CYBERSECURITY – THREATS & ATTACKS

1.	Compromises to intellectual property	Piracy, copyright infringement
2.	Software attacks	Viruses, worms, macros, denial of
3.	Deviations in quality of service	ISP, power, or WAN service issues
4.	Espionage or trespass	Unauthorized access and/or data
5.	Forces of nature	Fire, flood, earthquake, lightning
6.	Human error or failure	Accidents, employee mistakes
7.	Information extortion	Blackmail, information disclosure
8.	Missing, inadequate, or incomplete	Loss of access to information systems due to disk drive failure without
9.	Missing, inadequate, or incomplete	Network compromised because no
10.	Sabotage or vandalism	Destruction of systems or information
11.	Theft	Illegal confiscation of equipment or
12.	Technical hardware failures or errors	Equipment failure
13.	Technical software failures or errors	Bugs, code problems, unknown
14.	Technological obsolescence	Antiquated or outdated technologies

Table 2-1 consists of fourteen general categories that represent clear and present dangers to an organization’s people, information, and systems. Each organization must prioritize the threats it faces, based on the particular security situation in which it operates, its organizational strategy regarding risk, and the exposure levels at which its assets operate.

2.1 Intellectual Property

Intellectual property is 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.” Intellectual property can be trade secrets, copyrights, trademarks, and patents.

The unauthorized appropriation of IP constitutes a threat to information security. Employees may have access privileges to the various types of IP, and may be required to use the IP to conduct day-to-day business. Organizations often purchase or lease the IP of other organizations, and must abide by the purchase or licensing agreement for its fair and responsible use. The most common IP breach is the unlawful use or duplication of software-based intellectual property, more commonly known as **software piracy**.

Software licenses are strictly enforced by a number of regulatory and private organizations, and software publishers use several control mechanisms to prevent copyright infringement. In addition to the laws
against software piracy, two watchdog organizations investigate allegations of software abuse: the Software & Information Industry Association (SIIA) at *www.siia.net*, formerly known as the Software Publishers Association, and the Business Software Alliance (BSA) at *www.bsa.org*. A BSA survey in May 2006 revealed that as much as a third of all software in use globally is pirated.

A number of technical mechanisms—digital watermarks and embedded code, copyright codes, and even the intentional placement of bad sectors on software media—have been used to enforce copyright laws. The most common tool, a license agreement window that usually pops up during the installation of new software, establishes that the user has read and agrees to the license agreement. Another effort to combat piracy is the online registration process. Individuals who install software are often asked or even required to register their software to obtain technical support or the use of all features.

2.2 Software Attacks

Software attacks occur when an individual or group designs and deploys software to attack a system. Most of this software is referred to as **malicious code** or **malicious software**, or sometimes **malware**. These software components or programs are designed to damage, destroy, or deny service to the target systems. Some of the more common instances of malicious code are viruses and worms, Trojan horses, logic bombs, and back doors.

2.2.1 Virus

A computer **virus** consists of segments of code that perform malicious actions. The code attaches itself to an existing program and takes control of that program's access to the targeted computer. The virus-controlled target program then carries out the virus's plan by replicating itself into additional targeted systems. Many times users unwittingly help viruses get into a system. Opening infected e-mail or some other seemingly trivial action can cause anything from random messages popping up on a user’s screen to the complete destruction of entire hard drives of data. When these viruses infect a machine, they may immediately scan the local machine for e-mail applications, or even send themselves to every user in the e-mail address book.

One of the most common methods of virus transmission is via e-mail attachment files. Most organizations block e-mail attachments of certain types and also filter all e-mail for known viruses. In earlier times, viruses were slow-moving creatures that transferred viral payloads through the cumbersome movement of diskettes from system to system. Now, computers are networked, and e-mail programs prove to be fertile ground for computer viruses unless suitable controls are in place. The current software marketplace has several established vendors, such as Symantec Norton Anti-Virus and McAfee VirusScan, that provide applications to assist in the control of computer viruses.

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, spread sheets,and database applications, and the **boot virus**, which infects the key operating system files located in a computer’s boot sector.

2.2.2 Worms

A **worm** is a malicious program that replicates itself constantly, without requiring another program environment. Worms can continue replicating themselves until they completely fill available resources, such as memory, hard drive space, and network bandwidth.

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, so that 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, placing working copies of the worm code onto the server so that users of those shares are likely to become infected.

2.2.3 Trojan Horses

Trojan horses are software programs that hide their true nature and reveal their designed behaviour only when activated. Trojan horses are frequently disguised as helpful, interesting, or necessary pieces of software, such as readme.exe files often included with shareware or freeware packages.

2.2.4 Back Door or Trap Door

A virus or worm can have a payload that installs a **backdoor** 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 Subseven and Back Orifice.

2.2.5 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.

2.3 Deviations in Quality of Service

An organization's information system depends on the successful operation of many interdependent support systems, including power grids, telecom networks, parts suppliers, service vendors, and even the janitorial staff and garbage haulers. Any one of these support systems can be interrupted by storms, employee illnesses, or other unforeseen events.Deviations in quality of service can result from incidents such as a backhoe taking out a fiber-optic link for an ISP. 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.

.

2.4 Espionage or Trespass

When an unauthorized individual gains access to the information an organization is trying to protect, that 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 quite legal, for example, using a Web browser to perform market research. These legal techniques are called, collectively, **competitive intelligence**. When information gatherers employ techniques that cross the threshold of what is legal or ethical, they are conducting **industrial espionage**.

Some forms of espionage are relatively low tech. One example, called **shoulder surfing**. This technique is used in public or semi public settings when individuals gather information they are not authorized to 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 or subway where people use smartphones and tablet PCs, orother places where a person is accessing confidential information.

Acts of **trespass** can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems they have not been 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. These control methods and technologies employ multiple layers or factors to protect against unauthorized access.

The classic perpetrator of espionage or trespass is the hacker. **Hackers** are "people who use and create computer software [to] gain access to information illegally." There are generally two skill levels among hackers. The first is the **expert hacker**, or **elite hacker**, who develops software scripts and program exploits used by those in 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.

Expert hackers, dissatisfied with attacking systems directly, have turned their attention to writing software. These programs are automated exploits that allow novice hackers to act as **script kiddies**—hackers of limited skill who use expertly written software to attack a system—or **packet monkeys**—script kiddies who use automated exploits to engage in distributed denial-of-service attacks (described later in this chapter). The good news is that if an expert hacker can post a script tool where a script kiddie or packet monkey can find it, then systems and security administrators can find it, too.

The term **cracker** is now commonly associated with an individual who *cracks* or removes software protection that is designed to prevent unauthorized duplication. 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.

2.5 Forces of Nature

Forces of nature 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.

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.

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.

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.

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.

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.

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.

Hurricane or typhoon: A severe tropical cyclone originating in the equatorial regions of the Atlantic Ocean or Caribbean Sea or eastern regions of the Pacific Ocean (typhoon), traveling north, northwest, or northeast from its point of origin, and usually involving heavy rains. These storms can directly damage all or part of the information system or, more likely, the building that houses it. Organizations located in coastal or low-lying areas may experience flooding (see above). These storms may also 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.

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.

Electrostatic discharge (ESD):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.

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.

2.6 Human Error: 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. For example, a simple keyboarding error can cause worldwide Internet outages.

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. This is because employee mistakes can easily lead to the following: revelation of classified data, entry of erroneous data, accidental deletion or modification of data, storage of data in unprotected areas, and failure to protect information.

Leaving classified information in unprotected areas, such as on a desktop, on a Web site, or even in the trash can, is as much a threat to the protection of the information as is the individual who seeks to exploit the information, because one person's carelessness can create a vulnerability and thus an opportunity for an attacker. However, if someone damages or destroys data on purpose, the act belongs to a different threat category.

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. An example of the latter is the performance of key recovery actions in PKI systems. Many military applications have robust, dual-approval controls built

in. Some systems that have a high potential for data loss or system outages use expert systems to monitor human actions and request confirmation of critical inputs.

2.7 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. For example, Web-based retailer CD Universe was the victim of a theft of data files containing customer credit card information.

2.8 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.

2.9 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.

2.10 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. Vandalism to a Web site can erode consumer confidence, thus diminishing an organization's sales and net worth, as well as its reputation.

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.

2.11 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.

2.12 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.

2.13 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.

2.14 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.

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 (1) 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; (2) 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.” Each of these hidden code components can be used to collect information from or about the user which could then be used in a social engineering or identity theft attack.

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.

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. 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.

Password Crack

Attempting to reverse-calculate a password is often called **cracking**. A cracking attack is a component of many dictionary attacks (to be covered shortly). 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.

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**.

Dictionary

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

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.

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.

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.

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.

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. 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.

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.**

Social Engineering

In the context of information security, **social engineering** is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker. 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. For instance, anyone can check a company's Web site, or even call the main switchboard to get the name of the CIO; an attacker may then obtain even more information by calling others in the company and asserting his or her (false) authority by mentioning the CIO's name. Social engineering attacks may involve individuals posing as new employees or as current employees requesting assistance to prevent getting fired.

Another social engineering attack called the advance-fee fraud (AFF), and internationally known as the 4-1-9 fraud, is named after a section of the Nigerian penal code. The Perpetrators of 4-1-9 schemes often name fictitious companies, such as the Nigerian National Petroleum Company.

Phishing

Phishing is an attempt to gain personal or financial information from an individual, usually by posing as a legitimate entity.A variant is **spear phishing**, a label that applies to any highly targeted phishing attack. While normal phishing attacks target as many recipients as possible, a spear phisher sends a message that appears to be from an employer, a colleague, or other legitimate correspondent,to a small group or even one specific person. This attack is sometimes used to target those who use a certain product or Web site.

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**.”

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.