UNIT-1

Understanding Cyber Security

Learning Outcomes
By the end of this unit the learner will be able to:
✓ Define cyber security and its primary objectives ✓ Understand the various causes of cybercrime and those responsible for threats to cyber security ✓ Discuss the classifications of cyber crime and Microsoft's 10 laws of computer security

Unit 1

Understanding Cyber Security

What is Cyber Security?

Cyber security is the name for the safeguards taken to avoid or reduce any disruption from an attack on data, computers or mobile devices. Cyber security covers not only safeguarding confidentiality and privacy, but also the availability and integrity of data, both of which are vital for the quality and safety of care. Security breaches can occur when we use paper records, send information using fax machines and even verbally. However, the consequences of security breaches with digital information are potentially far more severe, as information can be distributed more easily and to a far wider audience.

Cyber-breaches are costly – in terms of expense, recovery time and through damage to reputation. In a Government Cyber Breaches Survey in 2017, 46% of businesses reported a cyber-breach or attack. That is why cyber security is a high priority for business and why all staff must be aware of how to implement protective measures. Individuals should also be aware of basic cyber security safeguards for personal use and when participating in the management and coordination of their care and support.

Importance of Security

The Internet has undoubtedly become the largest public data network, enabling and facilitating both personal and business communications worldwide. The volume of traffic moving over the Internet, as well as corporate networks, is expanding exponentially every day. More and more communication is taking place via e-mail; mobile workers, telecommuters, and branch offices are using the Internet to remotely connect to their corporate networks; and commercial transactions completed over the Internet, via the World Wide Web, now account for large portions of corporate revenue.

While the Internet has transformed and greatly improved the way we do business, this vast network and its associated technologies have opened the door to an increasing number of security threats from which corporations must protect themselves. Although network attacks are presumably more serious when they are inflicted upon businesses that store sensitive data, such as personal medical or financial records, the consequences of attacks on any entity range from mildly inconvenient to completely debilitating—important data can be lost, privacy can be violated, and several hours, or even days, of network downtime can ensue.

In addition to protecting their customers, corporations must protect their employees and partners from security breaches. The Internet, intranets, and extranets enable fast and effective communication between employees and partners. However, such communication and efficiency can of course be impeded by the effects of a network attack. An attack may directly cause several hours of

downtime for employees, and networks must be taken down in order for damage to be repaired or data to be restored. Clearly, loss of precious time and data can greatly impact employee efficiency and morale.

For the purposes of computer security, there are two types of people, insiders (employees) and outsiders (nonemployees). Figure.1.1 shows the three classes of computer security and crime caused by each of the two types plus the special class of threats that are not directly caused by humans, namely accidents.

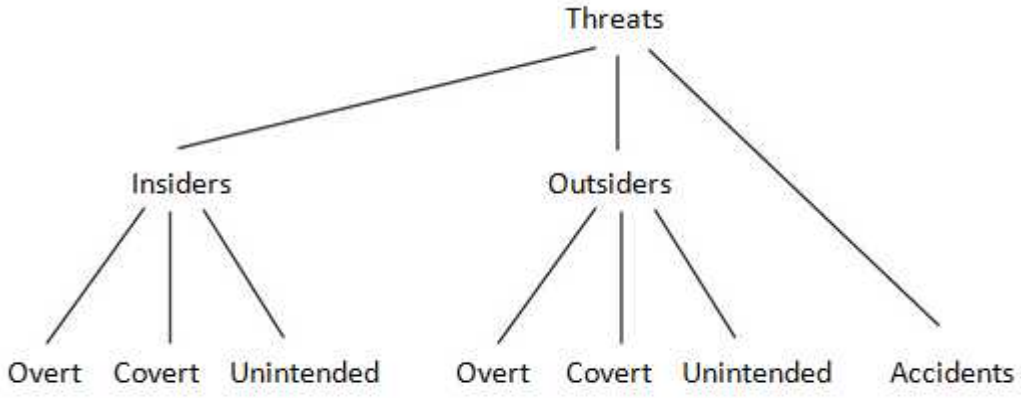


Fig. 1.1

The seven classes are as follows:

1. Insiders overt. Overt actions by insiders are often performed by disgruntled employees and result in destruction of data and equipment. However, this class is small compared to the other six.
2. Insiders covert. Generally, insiders have more information about a place of work than outsiders, which is why they can wreak more havoc. Thus, this class corresponds to serious threats and criminal actions.
3. Insiders unintended. Employees make errors and can also neglect their duties. Consequently, this class encompasses actions such as wrong inputs, wrong data, damage as a result of extreme temperatures or other harsh conditions, and interruption of vital services.
4. Outsiders overt. Physical attacks on computer and network facilities belong in this class as are also DoS attacks.
5. Outsiders covert. This wide class consists of the various types of rogue software sent from the outside to a personal computer or to a large computer facility.
6. Outsiders unintended. It is fairly rare that an outsider will harm a computer or data unintentionally.
7. Finally, there are accidents. They always happen, not just in the computing field. Accidents are caused either by nature, such as earthquake or flood, or indirectly byhumans

There are many different types of computer security threats and problems, but they can be classified into three large classes as follows:

- Physical security. A personal computer can be stolen. A large computer center can be broken into and equipment taken. Fire, electrical surges, and floods can damage computer hardware and network connections and cause loss of data.
- Rogue software. We have all heard of computer viruses. Small, sneaky programs that invade our computers and spread quickly and silently. Viruses are just one aspect of the general threat posed by rogue software.
- Most computers are connected to networks, and most local networks are connected to the Internet. Thus, there is a large class of computer security threats that are related to networks and fall under the category of network security. This wide area of security includes threats such as port scanning, spoofing, password cracking, spyware, and identity theft.

1. If someone can persuade you to run his program on your computer, it's not your computer anymore.
2. If someone can alter the operating system on your computer, it's not your computer anymore.
3. If someone has unrestricted physical access to your computer, it's not your computer anymore.
4. If you allow someone to upload programs to your website, it's not your website anymore.
5. Weak passwords defeat strong security.
6. A computer is only as secure as its owner/user is trustworthy.
7. Encrypted data is only as secure as the decryption key.
8. An out-of-date virus scanner is only marginally better than none at all.
9. Absolute anonymity isn't practical, in real life or on the Web.
10. Technology is not a panacea.

Physical Security

What normally comes to mind, when hearing about or discussing computer security, is either viruses or some of the many security issues that have to do with networks, such as loss of privacy, identity theft, or how to secure sensitive data sent on a network. Computer security, however, is a vast discipline that also includes mundane topics such as how to physically protect computer equipment and secure it against fire, theft, or flood.

Physical Threats

Surges in electrical power, often caused by lightning, may burn out electronic components in the computer. Solution: Use an uninterruptible power supply (UPS). Such a device regulates the incoming voltage and produces a clean output signal. If the voltage gets high, the UPS trims it. If the voltage drops, the UPS uses its internal battery to supply the computer with power for a few minutes, enough to either turn off the computer (typical for a home computer) or to start a generator (typical in a large installation, especially an installation that has to operate continuously, such as a hospital or a telephone exchange).

Physical security of computer facilities. We constantly hear of damage done by computer viruses and other malicious programs, but the best virus protection software cannot prevent a home personal computer from being stolen Thus, computer security starts by protecting the facilities that house computers and computer data. This problem is especially acute in industry. Many a company can be wiped out if its computers or especially if its sensitive data are stolen or damaged. Damage can be intentional, inflicted by a criminal or a disgruntled employee, or accidental, caused by fire, power failure, or broken air conditioning.

The solution is to physically protect this sensitive asset. A home should have an alarm system and power to the computer should go through an uninterrupted power supply (UPS). A commercial entity should have a secure computer facility, with controlled access, heavy doors, card-operated locks, security cameras, and an automatic fire system. In addition, special care should be given to unconventional entry points, such as attics and air conditioning ducts. A modern office building often has a large attic above the ceiling of each floor. This space is handy for stringing wires inside the building, but can be used by a person to crawl into an otherwise secure room. A wide air-conditioning duct can be used for the same purpose and should therefore be secured by a heavy screen.
Other items, such as emergency lights, fireproof containers (for storing disks and papers), and proper training of personnel, are also important.

- Traditionally, fire is suppressed by water, but this causes damage to structures and equipment that may exceed the damage caused by the fire.Heat is only one type of damage caused by a fire. Smoke and soot particles resulting from a fire can compound the damage by contaminating removable disks, ruining the delicate mechanisms of magnetic disk and optical drives, and dirtying the electrical connections in keyboards

- Theft should especially be mentioned, because personal computers are getting smaller and lightweight all the time and are therefore easy to steal.
- A facility that uses electronic locks and keys or other physical-identification devices to restrict access to certain areas should consider the following problem, known as piggybacking or tailgating. An intruder may wait at a locked door, perhaps holding disks, paper or other innocuous-looking stuff with both hands, trying to look legitimate and waiting for the door to open. When someone comes out of the restricted room, the intruder slips in while the door is still open. A guard can prevent such a problem, but this is an expensive solution. An alternative is to install a turnstile, or even a mantrap. The latter device is a two-door entrance where a person has to pass through two doors in order to enter or exit a restricted room. To enter, a person must pass through door A to a small space, the mantrap, and then open door B to the restricted room. The point is that door B will not open until door A is fully closed.

User tracking

Imagine a facility with many computers and many workers, where a user may perform a task on a computer, move away to do something else, then step to the nearest computer to perform another task. A good example is a hospital with doctors and nurses treating patients and updating patient records all the time. Another example is a lab where tests (perhaps blood tests or forensic tests) are performed by workers, and a worker has to enter the results of a test into a computer.

In such a situation, it is important to keep track of which employee used what computer, when and for what purpose. The simplest solution is to assign each user a password. The user has to log into the computer, perform a task, then log off. In the hospital example, where emergencies may and do occur often, such a procedure is too time consuming and unrealistic.

A more sophisticated solution is to provide each user with a special, unique identification card (a key) and install in each computer special hardware (a lock) that can recognize such cards. The lock and key communicate by means of low-power radio transmissions, and each key contains a large (typically 32 bits) identification code. When a user arrives at a computer and starts using it, the lock recognizes the code on the key and immediately logs the user on. When the user walks away, the lock senses the loss of contact and immediately logs the user off. When no user is logged on, the computer cannot be used.

Physical Protection of Data

Data is normally stored on devices that are easily damaged or destroyed. Paper, magnetic disks, CDs and DVDs are sensitive to fire, magnetic fields, or scratches. Data stored on such devices deteriorates even under ideal storage conditions. Thus, data has to be physically protected, and this can be achieved by backing up sensitive data periodically, so a fresh backup is always at hand. A home computer should have two external disks (or rewritable CDs or DVDs), one kept at home and the other kept in a different location, such as a friend’s home.

A company that depends on its digital data should also back it up on a regular basis, but may often use its local area network for this task. Data from an office or location A may be sent through the local network to another office B where it is stored as a backup, while at the same time data from B may be backed up in A.

In general, a computer user, whether an individual or an organization, should have a disaster-recovery plan based on regular and complete data backups. The plan should specify what to do if all the physical facilities are destroyed. New facilities may have to be rented in a hurry, new computers may have to be purchased or rented immediately, and all the lost data restored from backups. Experience shows that a detailed disaster-recovery plan may help even a large organization, such as a bank, recover from a terrible disaster (fire, earthquake, flood, terrorism, computer virus) in a short period of time.

Hard copy. The media has been touting the paperless office for several decades, but we still use paper. In fact, we use it more and more. Security workers know that criminals often collect papers thrown away carelessly and scrutinize them for sensitive information such as credit card numbers and passwords to computer accounts. This behavior is part of the general practice of dumpster diving. The solution is to shred sensitive documents, and even not-so-sensitive papers.

What is Cyber Crime?

The term cyber crime is used to describe a unlawful activity in which computer or computing devices such as smartphones, tablets, Personal Digital Assistants(PDAs), etc. which are stand alone or a part of a network are used as a tool or/and target of criminal acitivity. It is often commited by the people of destructive and criminal mindset either for revenge, greed or adventure.

Classification of Cyber Crimes

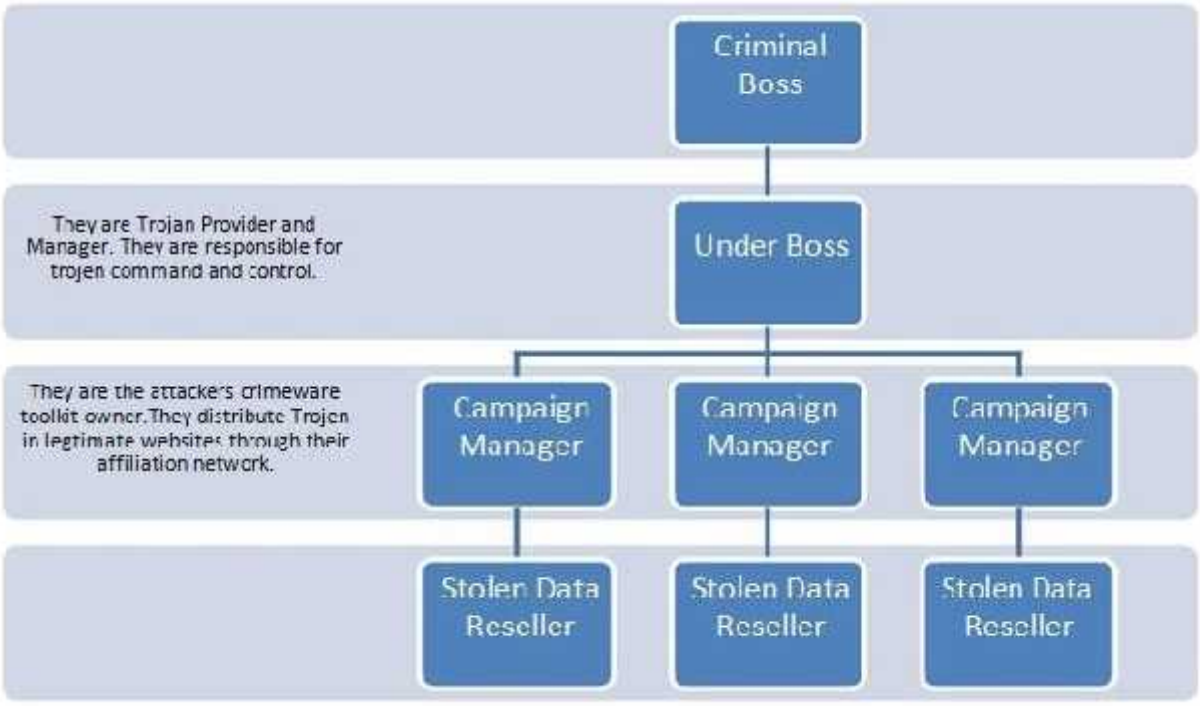
The cyber criminal could be internal or external to the organization facing the cyber attack.
Based on this fact, the cyber crime could be categorized into two types:

- Insider Attack: An attack to the network or the computer system by some person with authorized system access is known as insider attack. It is generally performed by dissatisfied or unhappy inside employees or contractors. The motive of the insider attack could be revenge or greed. It is comparitively easy for an insider to perform a cyber attack as he is well aware of the policies, processes, IT architecture and wealness of the security system. Moreover, the attacker have an access to the network. Therefore it is comparatively easy for a insider attacker to steel sensitive information, crash the network, etc. In most of the cases the reason for insider attack is when a employee is fired or assigned new roles in an organization, and the role is not reflected in the IT policies. This opens a vernability window for the attacker. The insider attack could be prevented by planning and installing an Internal intrusion detection systems (IDS) in the organization.

- External Attack: When the attacker is either hired by an insider or an external entity to the organization, it is known as external attack. The organization which is a victim of cyber attack not only faces financial loss but also the loss of reputation. Since the attacker is external to the organization, so these attackers usually scan and gathering information.An expreicend network/security administrator keeps regual eye on the log generated by the firewalls as extertnal attacks can be traced out by carefully analysinig these firewall logs. Also, Intrusion Detection Systems are installed to keep an eye on external attacks.

The cyber attacks can also be classified as structure attacks and unstructured attacks based on the level of maturity of the attacker. Some of the authors have classified these attacks as a form of external attacks but there is precedence of the cases when a structured attack was performed by an internal employee. This happens in the case when the competitor company wants the future strategy of an organization on certain points. The attacker may strategically gain access to the company as an employee and access the required information.

Cyber crimes have turned out to be a low-investment, low-risk business with huge returns. Now-a-days these structured crimes are performed are highly organized. There is a perfect hierarchical organizational setup like formal organizations and some of them have reached a level in technical capabilities at par with those of developed nation. They are targeting large financial organizations, defence and nuclear establishments and they are also into online drugs trading.



Reasons for Commission of Cyber Crimes

There are many reasons which act as a catalyst in the growth of cyber crime. Some of the prominent reasons are:

a. Money: People are motivated towards committing cyber crime is to make quick and easy money.
b. Revenge: Some people try to take revenge with other person/organization/society/ caste or religion by defaming its reputation or bringing economical or physical loss. This comes under the category of cyber terrorism.
c. Fun: The amateur do cyber crime for fun. They just want to test the latest tool they have encountered.
d. Recognition: It is considered to be pride if someone hack the highly secured networks like defense sites or networks.

e. Anonymity- Many time the anonymity that a cyber space provide motivates the person to commit cyber crime as it is much easy to commit a cyber crime over the cyber space and remain anonymous as compared to real world.It is much easier to get away with criminal activity in a cyber world than in the real world. There is a strong sense of anonymity than can draw otherwise respectable citizens to abandon their ethics in pursuit personal gain.
f. Cyber Espionage: At times the government itself is involved in cyber trespassing to keep eye on other person/network/country. The reason could be politically, economically socially motivated.

Kinds of Cyber Crime

Various types of cyber crimes are:

Cyber Stalking

It is an act of stalking, harassing or threatening someone using Internet/computer as a medium. This is often done to defame a person and use email, social network, instant messenger, web-posting, etc. as a using Internet as a medium as it offers anonymity. The behaviour includes false accusations, threats, sexual exploitation to minors, monitoring, etc.

Forgery and Counterfeiting

It is a use of computer to forgery and counterfeiting is a document. With the advancement in the hardware and the software, it is possible to produce counterfeit which matches the original document to such an extent that it is not possible to judge the authenticity of the document without expert judgement.

Software Piracy and Crime related to IPRs

Software piracy is an illegal reproduction and distribution for personal use or business. It comes under crime related to IPR infringement. Some of the other crimes under IPR infringement are: download of songs, downloading movies, etc.

Cyber Terrorism

It is defined as the use of computer resources to intimidate or coerce government, the civilian population or any segment thereof in furtherance of political or social objectives.

Phishing

It is a process of acquiring personal and sensitive information of an individual via email by disguising as a trustworthy entity in an electronic communication. The purpose of phishing is identity theft and the personal information like username, password, and credit card number etc. may be used to steal money from user account. If a telephone is used as a medium for identity theft, it is known as Vishing (voice phishing). Another form of phishing is Smishing, in which sms is used to lure customers.

Computer Vandalism

It is an act of physical destroying computing resources using physical force or malicious code.

Computer Hacking

It is a practice of modifying computer hardware and software to accomplish a goal outside the creator‟s original purpose. The purpose of hacking a computer system may vary from simply demonstrations of the technical ability, to sealing, modifying or destroying information for social, economic or political reasons. Now the corporate are hiring hackers, a person who is engaged in hacking computers, to intentionally hack the computer of an organization to find and fix security vulnerabilities.

The hackers may be classified as:

- White Hat: white hat hackers are the persons who hack the system to find the security vulnerabilities of a system and notify to the organizations so that a preventive action can be taken to protect the system from outside hackers. White hat hackers may be paid employee of an organization who is employed to find the security loop-holes, or may be a freelancer who just wants to prove his mantle in this field. They are popular known as ethical hackers.
- Black Hat: in contrast to the white hat, the black hat hack the system with ill intentions. They may hack the system for social, political or economically motivated intentions. They find the security loopholes the system, and keep the information themselves and exploit the system for personal or organizational benefits till organization whose system is compromised is aware of this, and apply security patches. They are popularly known as crackers.
- Grey Hat: Grey hat hackers find out the security vulnerabilities and report to the site administrators and offer the fix of the security bug for a consultancy fee.
- Blue hat: A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch, looking for exploits so they can be closed.

Creating and distributing viruses over internet

The spreading of an virus can cause business and financial loss to an organization. The loss includes the cost of repairing the system, cost associated with the loss of business during downtime and cost of loss of opportunity. The organization can sue the hacker, if found, for the sum of more than or equivalent to the loss borne by the organization.

Spamming

Sending of unsolicited and commercial bulk message over the internet is known as spamming.

An email can be classified as spam, if it meets following criteria:

I. Mass mailing:- the email is not targeted to one particular person but to a large number of peoples.
II. Anonymity:- The real identify of the person not known
III. Unsolicited:- the email is neither expected nor requested for the recipient.

These spams not only irritate the recipients and overload the network but also waste the time and occupy the valuable memory space of the mailbox.

Cross Site Scripting

It is an activity which involves injecting a malicious client side script into a trusted website. As soon as the browser executes the malicious script, the malicious script gets access to the cookies and other sensitive information and sent to remote servers. Now this information can be use to gain financial benefit or physical access to a system for personal interest.

Online Auction Fraud

There are many genuine websites who offers online auction over internet. Taking the advantage of the reputation of these websites, some of the cyber criminals lure the customers to online auction fraud schemes which often lead to either overpayment of the product or the item is never delivered once the payment is made.

Cyber Squatting

It is an act of reserving the domain names of someone else‟s trademark with intent to sell it afterwards to the organization who is the owner of the trademark at a higher price.

Logic Bombs

These are malicious code inserted into legitimate software. The malicious action is triggered by some specific condition. If the conditions holds true in future, the malicious action begins and based on the action defined in the malicious code, they either destroy the information stored in the system or make system unusable.

Web Jacking

The hacker gain access to a website of an organization and either blocks it or modify it to serve political, economical or social interest.

Internet Time Thefts

Hacking the username and password of ISP of an individual and surfing the internet at his cost is Internet Time Theft.

Denial of Service Attack

It is a cyber attack in which the network is chocked and often collapsed by flooding it with useless traffic and thus preventing the legitimate network traffic.

Data Diddling

It is a practice of changing the data before its entry into the computer system. Often, the original data is retained after the execution on the data is done. For example, DA or the basic salary of the person is changed in the payroll data of an individual for pay calculation. Once the salary is calculated and transferred to his account, the total salary is replaced by his actual salary in the report.

Email Spoofing

It is a process of changing the header information of an e-mail so that its original source is not identified and it appears to an individual at the receiving end that the email has been originated from source other than the original source.

Further Reading:

- ✓ ***Cybersecurity for Beginners, May'2015 by Book by Raef Meeuwiss***
- ✓ ***Cybersecurity ??? Attack and Defense Strategies: Infrastructure Security Jan'2018 by Erdal Ozkaya and Yuri Diogenes***