DIGITAL NOTES

OF

CYBER SECURITY
(R20A6202)

B. TECH IV YEAR – I SEM

(2024-25)

PREPARED BY

V.V. NAGAMANI

K. KOUSHIL REDDY

G. LIKITHA

DEPARTMENT OF INFORMATION TECHNOLOGY

MALLA REDDY COLLEGE OF ENGINEERING & TECHNOLOGY

(Autonomous Institution – UGC, Govt. of India)

Recognized under 2(f) and 12 (B) of UGC ACT 1956

(Affiliated to JNTUH, Hyderabad, Approved by AICTE - Accredited by NBA & NAAC – 'A' Grade - ISO 9001:2015 Certified)

Maisammaguda, Dhulapally (Post Via. Hakimpet), Secunderabad – 500100, Telangana State, India

MALLA REDDY COLLEGE OF ENGINEERING AND TECHNOLOGY

IV Year B.Tech. IT- I Sem **L/T/P/C**
3/-/-/ 3

CYBER SECURITY

(R20A6202)

COURSE OBJECTIVES:

1. To understand the basic concepts of cybercrimes.
2. To study different attacks in cybercrimes.
3. To understand the cyber security trends and measures in mobile and wireless devices.
4. To understand different tools and methods used in cybercrime.
5. To study cyber security challenges and implications.

UNIT - I

Introduction to Cyber Security: Basic Cyber Security Concepts, layers of security, Vulnerability, threat, Harmful acts, Internet Governance – Challenges and Constraints, Computer Criminals, CIA Triad, Assets and Threat, motive of attackers, active attacks, passive attacks, Software attacks, hardware attacks, Spectrum of attacks, Taxonomy of various attacks, IP spoofing, Methods of defense, Security Models, risk management, Cyber Threats- Cyber Warfare, Cyber Crime, Cyber terrorism, Cyber Espionage, etc., Comprehensive Cyber Security Policy.

UNIT - II

Cyberspace and the Law & Cyber Forensics: Introduction, Cyber Security Regulations, Roles of International Law. The INDIAN Cyberspace, National Cyber Security Policy. Introduction, Historical background of Cyber forensics, Digital Forensics Science, The Need for Computer Forensics, Cyber Forensics and Digital evidence.

UNIT - III

Cybercrime: Mobile and Wireless Devices: Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for Organizations, Organizational Measures for Handling Mobile , Organizational Security Policies and Measures in Mobile Computing Era , Laptops.

UNIT - IV

Cyber Security: Organizational Implications: Introduction cost of cybercrimes and IPR issues, web threats for organizations, security and privacy implications, social media marketing: security risks and perils for organizations, social computing and the associated challenges for organizations. **Cybercrime and Cyber terrorism**: Introduction, intellectual property in the cyberspace, the ethical dimension of cybercrimes the psychology, mindset and skills of hackers and other cybercriminals.

UNIT - V

Privacy Issues: Basic Data Privacy Concepts: Fundamental Concepts, Data Privacy Attacks, Data linking and profiling, privacy policies and their specifications, privacy policy languages, privacy indifferent domains- medical, financial ,,etc.

Cybercrime: Examples and Mini-Cases

Mini-Cases: The Indian Case of online Gambling, An Indian Case of Intellectual Property Crime, Financial Frauds in Cyber Domain.

TEXT BOOKS*:*

1. Nina Godbole and Sunit Belpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley
2. B. B. Gupta, D. P. Agrawal, Haoxiang Wang, Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335, 2018.

REFERENCE BOOKS:

1. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press.
2. Introduction to Cyber Security , Chwan-Hwa(john) Wu,J.David Irwin.CRC PressT&FGroup

COURSE OUTCOMES:

Student will be able to

- Analyze threats and risks within context of the cyber security.
- Understand different attacks in cyber world.
- Recognize trends and risk involved with mobile and wireless devices.
- Expose to tools and methods used in cyber crimes.
- Evaluate organizations challenges and implications with respect tocyber security.

INDEX

UNIT-I

Introduction to Cyber Security

Basics cyber security concepts:

Cyber Security is referred to the security offered through online services to protect the online information.

With an increasing amount of people getting connected to the Internet, the security threats are also massively increasing.

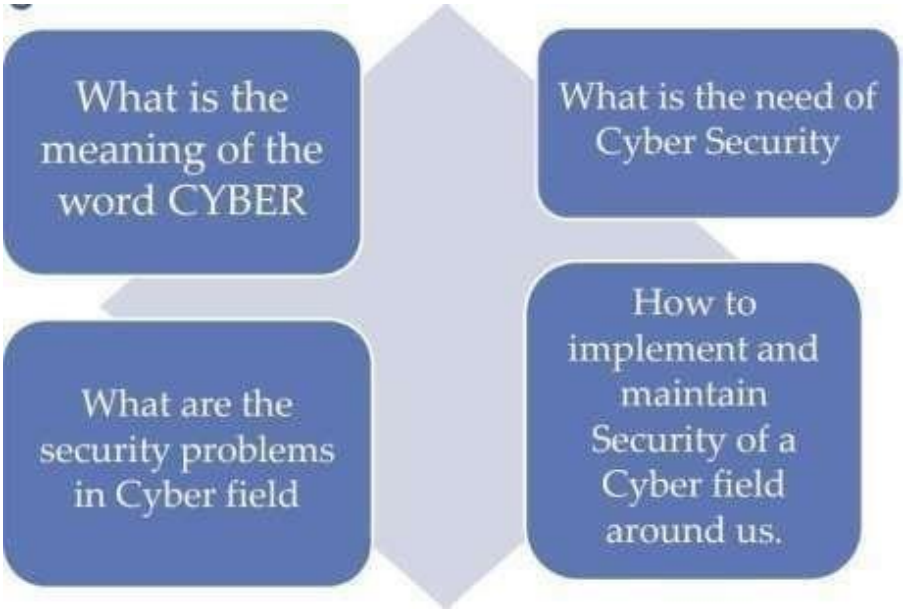
Cyber Security:

It is the body of technologies, processes and practices designed to protect networks, devices, programs and data from attack, theft, damage, modification or unauthorized access. It is also called as **Information Technology Security**.

OR

Cyber Security is the setoff principles and practices designed to protect the computing resources and online information against threats.

Understanding Cyber Security:



Security Problems & Maintaining Security in Cyber field:

Viruses & Worms:

A virus is a program that is loaded into the computer without user's knowledge and runs against the user's wish.

Maintenance:

Install a security suite that protects the computer against threats such as viruses and worms. (eg., Antivirus)

Hackers:

A hacker is a person who uses computers to gain unauthorized access to data.

Types of Hackers:

- **Black Hat Hackers:** (Unethical Hacker or Security Cracker)

  These people hack the system illegally to steal money or to achieve their own illegal goals. They find the banks or organization with weak security and steal money or credit card information, theycan also modifyor destroyconfidential data.

- **White Hat Hackers:** (Ethical Hacker or Penetration Tester)

  These people use the same technique used by the black hat hackers, but they can only hack the system that theyhave permission to hack inorder to test the securityof the system.

  They focus on securing and protecting IT System. White Hat Hacker is legal.

- **Grey Hat Hackers:**

  GreyHat Hackers are hybrid of Black hat hackers & White hat hackers

  They can hack any system even if they don't have permission to test the security of the system but theywill never steal money or damage the system.

Maintenance:

It may be impossible to prevent computer hacking, however effective security controls including strong passwords and the use of firewalls.

Malware: (MALicious softWARE)

Malware is any software that infects and damages a computer system without the owner's knowledge or permission.

Maintenance:

Download an anti-malware program that also helps prevent infection. Activate network protection firewall, antivirus.

Trojan Horse:

Trojan horse are email viruses that can duplicate themselves, steal information or harm the computer system. These viruses are the most serious threats to computers.

Maintenance:

Securitysuits such as Avast Internet Security, which will prevent from downloading Trojan Horses.

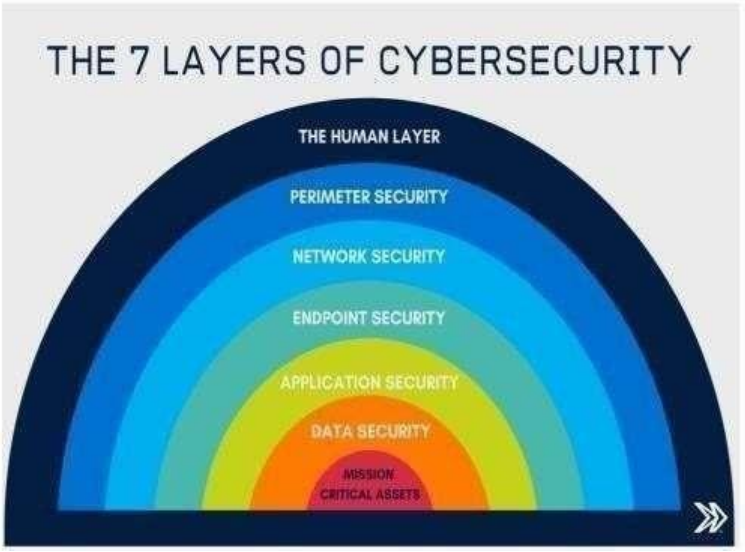
Password Cracking:

Password attacks are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas and social network sites.

Maintenance:

Use always strong password. Never use same password for two different sites.

LAYERS OF SECURITY



The 7 layers of cyber securityshould center on the mission critical assets.

1. **Mission Critical Assets:** This is the data which need to be protected.
2. **Data Security:** It protects the storage and transfer of data.
3. **Application Security:** It protects access to an application which handles the mission critical assets and internal securityof the application.
4. **Endpoint Security:** It protects the connection between devices and the network.
5. **Network Security:** It protects an organization's network to prevent unauthorized access of the network.
6. **Perimeter Security:** It includes both the physical and digital security methodologies that protect the overall business.
7. **The Human Layer:** Humans are the weakest link in any cyber security posture. Human security control includes phishing simulations and access management control that protect mission critical assets from a wide variety of human threats, including cyber criminals, malicious insiders and negligent users.

Vulnerability, Threats and Harmful Acts:

Vulnerabilities are the gaps or weaknesses in a system that make threats possible and tempt threat actors to exploit them.

Types of vulnerabilities in network security:

SQL injections,
Server misconfigurations,

Cross-site scripting, and Transmitting sensitive data in a non- encrypted plain text format.

Cyber threats are security incidents or circumstances with the potential to have a negative outcome for your network or other data management systems.

Examples:

Phishing attacks that result in the installation of **malware** that infects your data, failure of a staff member to follow data protection protocols that cause a **data breach**, or even a tornado that takes down your company's data headquarters, disrupting access. Vulnerabilities is not risk without a threat exploiting it. Threat is not a risk without a vulnerabilityto be exploited.

Internet Governance – Challenges and Constraints:

Internet Governance is defined as the development and application by Government. The private sector and civil sector in their respective roles of shared principles, norms, rules, decision making procedures and programs that shape the evolution and use of the Internet.

The definition developed by the Working Group of Internet Governance (WGIG) dates back to 2005, and has remained unchanged ever since then and is now a complex system involving a multitude of issues, actors, mechanisms, procedures and instruments.

Internet Governance Actors:

According to the definition, there is no single organization incharge of the Internet but various stakeholders – Governments, Inter Governmental Organizations, the private sector, the technical community and Civil Society share roles and responsibilities in shaping the evolution and use of this network.

There are multiple actors which are involved in one wayor another in the governance of Internet.

1. Internet Corporation for Assigned Names and Numbers (ICANN)
2. Internet Engineering Task Force (IETF)
3. International Telecommunication Union (ITU)
4. World Intellectual Property Organization (WIPO)
5. Internet Governance Forum (IGF)

Computer Criminals:

Computer crimes have quickly become one of the fastest rising forms of modern crime. According to cyber experts, approx., 1 million potential cyber-attacks are attempted per day.

Types of Cyber Criminals:

Cyber criminals are also known as hackers. Hackers are extremely difficult to identify on both individual and group level, due to their various security measures.

Cyber Security expert assert that Cyber Criminals are using more ruthless methods to achieve their objectives and the proficiency of attacks are expected to advance as they continue to develop new methods of cyber-attacks.

Identity Thieves:

Identity thieves are cyber criminals who try to gain access to their victim's personal information. They use their information to make financial transaction while impersonating their victims. Identitytheft is one of the oldest cybercrime.

Internet Stalkers:

Internet Stalkers are individuals who maliciously monitor the online activity of their victims to acquire personal information.

This form of cybercrime is conducted through the use of social networking platforms and malware, which are able to track an individual's computer activity with very little detection. Businesses should be aware of Internet Stalkers.

Phishing Scammers:

Phishing are cyber criminals who attempt to get hold of personal or sensitive information through victim's computer.

This is often done via phishing websites that are designed to copycat small business, corporateor government websites.

Once such information is obtained, phishers either use the information themselves for identity fraud scams or sell it in the dark web.

Cyber Terrorists:

Cyber Terrorism is a well-developed politically inspired cyber-attack in which the cyber criminal attempts to steal data or corrupt corporate or Government computer systems and networks resulting in harm to countries, business, organizations and even individuals.

The key difference between an act of cyber terrorism and a regular cyber-attack is that within an attack of cyber terrorism, hackers are politically motivated as opposed to just seeking financial gain.

CIA Triad

The CIA Triad is actually a security model that has been developed to help people think about various parts of IT security.

CIA triad broken down:

Confidentiality:

Protecting confidentiality is dependent on being able to define and enforce certain access levels for information. This process involves separating information into various collections that are organized by authorized user, who needs to access the information and how sensitive that information actually is - i.e. the amount ofdamage suffered if the confidentialitywas breached.

- Standard measures to establish confidentiality include:

Data Encryption

Two-factor authentication

Biometric Verification

SecurityTokens.

Integrity

This is an essential component of the CIA Triad and designed to protect data from deletion or modification from any unauthorized party, and it ensures that when an authorized person makes a change that should not have been made the damage can be reversed.

- Standard measures to guarantee Integrity include:

Cryptographychecksums

Using file permissions

Uninterrupted power supplies

Data backups.

Availability

This is the final component of the CIA Triad and refers to the actual availability of your data. Authentication mechanisms, access channels and systems all have to work properly for the information they protect and ensure it's available when it is needed.

- Standard measures to guarantee Availability include:

Backing up datato external drives

Implementing firewalls

Having backup power supplies

Data redundancy

Assets and Threat

An asset is any data, device or other component of an organization's systems that is valuable – often because it contains sensitive data or can be used to access such information. For example: An employee's desktop computer, laptop or company phone would be considered an asset, as would applications on those devices. Likewise, critical infrastructure, such as servers and support systems, are assets. An organization's most common assets are

information assets. These are things such as databases and physical files – i.e. the sensitive data that you store

A threat is any incident that could negatively affect an asset – for example, if it's lost, knocked offline or accessed by an unauthorized party.

- Threats can be categorized as circumstances that compromise the confidentiality, integrity or availabilityof an asset, and can either be intentional or accidental.
- Intentional threats include things such as criminal hacking or a malicious insider stealing information, whereas accidental threats generally involve employee error, a technical malfunction or an event that causes physical damage, such as a fire or natural disaster.

Motive of Attackers

The categories of cyber-attackers enable us to better understand the attackers' motivations and the actions they take. As shown in Figure, operational cyber security risks arise from three types of actions:

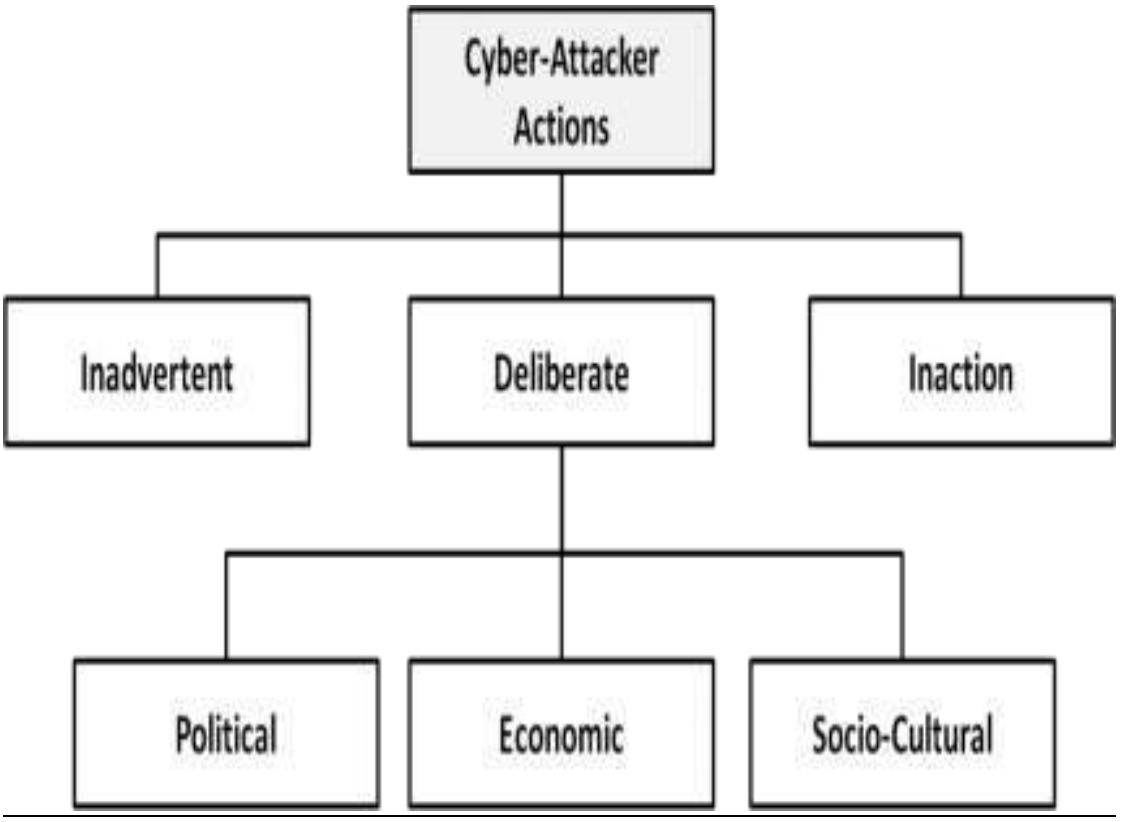
i) inadvertent actions (generally by insiders) that are taken without malicious or harmful intent;

ii) deliberate actions (by insiders or outsiders) that are taken intentionally and are meant to do harm; and

iii) inaction (generally by insiders), such as a failure to act in a given situation, either because of a lack of appropriate skills, knowledge, guidance, or availability of the

Correct person to take action Of primary concern here are deliberate actions, of which there are three categories ofmotivation.

1. ***Political motivations****:* examples include destroying, disrupting, or taking control of targets; espionage; and making political statements, protests, or retaliatoryactions.
2. ***Economic motivations****:* examples include theft of intellectual property or other economically valuable assets (e.g., funds, credit card information); fraud; industrial espionage and sabotage; and blackmail.
3. ***Socio-cultural motivations****:* examples include attacks with philosophical, theological, political, and even humanitarian goals. Socio-cultural motivations also include fun, curiosity, and a desire for publicityor ego gratification.


Cyber-Attacker Actions
Inadvertent
Deliberate
Inaction
Political
Economic
Socio-Cultural

Types of Cyber Attacks

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

Cyber-attacks can be classified into the following categories:

1) **Web-based attacks**
2) **System-based attacks**

Web-based attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-

1. Injection attacks

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Example- SQL Injection, code Injection, log Injection, XML Injection etc.

2. DNS Spoofing

DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attackers computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

3. Session Hijacking

It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

4. Phishing

Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthyentity in electronic communication.

5. Brute force

It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

6. Denial of Service

It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-

Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

Protocol attacks- It consumes actual server resources, and is measured in a packet. **Application layer attacks-** Its goal is to crash the web server and is measured in request per second.

7. Dictionary attacks

This type of attack stored the list of a commonly used password and validated them to get original password.

8. URL Interpretation

It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

9. File Inclusion attacks

It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

10. Man in the middle attacks

It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

System-based attacks

These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

2. Virus

It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

3. Worm

It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

4. Trojan horse

It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

5. Backdoors

It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

6. Bots

A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

Active attacks: An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target.

Types of Active attacks:

Masquerade: in this attack, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen login IDs and passwords, through finding security gaps in programs or through bypassing the authentication mechanism.

Session replay: In this type of attack, a hacker steals an authorized user's log in information by stealing the session ID. The intruder gains access and the ability to do anything the authorized user can do on the website.

Message modification: In this attack, an intruder alters packet header addresses to direct a message to a different destination or modifythe data on a target machine.

In a **denial of service (DoS)** attack, users are deprived of access to a network or web resource. This is generally accomplished by overwhelming the target with more traffic than it can handle.

In a **distributed denial-of-service (DDoS)** exploit, large numbers of compromised systems

(sometimes called a botnet or zombie army) attack a single target.

Passive Attacks:*Passive attacks* are relatively scarce from a classification perspective, but can be carried out with relative ease, particularly if the traffic is not encrypted.

Types of Passive attacks:

Eavesdropping (tapping): the attacker simply listens to messages exchanged by two entities. For the attack to be useful, the traffic must not be encrypted. Any unencrypted information, such as a password sent in response to an HTTP request, may be retrieved by the attacker.

Traffic analysis: the attacker looks at the metadata transmitted in traffic in order to deduce information relating to the exchange and the participating entities, e.g. the form of the exchanged traffic (rate, duration, etc.). In the cases where encrypted data are used, traffic analysis can also lead to attacks by cryptanalysis, whereby the attacker may obtain information or succeed in unencrypting the traffic.

Software Attacks:

Malicious code (sometimes called *malware*) is a type of software designed to take over or damage a computer user's operating system, without the user'sknowledge or approval. It can be very difficult to remove and very damaging. Commonmalware examples are listed in the following table:

Attack	Characteristics
Virus	A *virus* is a programthat attempts to damage a computer system and replicate itself to other computer systems. A virus: • Requires a host to replicate and usually attaches itself to a host file or a hard drive sector. • Replicates each time the host is used. • Often focuses on destruction or corruption of data. • Usuallyattaches to files with execution capabilities such as .doc, .exe, and .bat extensions. • Often distributes via e-mail. Many viruses can e-mail themselves to everyone in your address book. • Examples: Stoned, Michelangelo, Melissa, I Love You.

Worm	A *worm* is a self-replicating program that can be designed to do any number of things, such as delete files or send documents via e-mail. A worm can negatively impact network traffic just in the process ofreplicating itself. A worm: • Can install a backdoor in the infected computer. • Is usually introduced into the system through a vulnerability. • Infects one system and spreads to other systems on the network. • Example: Code Red.

Trojan horse	A *Trojan horse* is a malicious program that is disguised as legitimate software. Discretionary environments are often more vulnerable and susceptible to Trojan horse attacks because security is user focused and user directed. Thus the compromise of a user account could lead to the compromise of the entire environment. A Trojan horse: • Cannot replicate itself. • Often contains spying functions (such as a packet sniffer) or backdoor functions that allow a computer to be remotely controlled from the network. • Often is hidden in useful software such as screen savers or games. • Example: Back Orifice, Net Bus, Whack-a-Mole.
Logic Bomb	A *Logic Bomb* is malware that lies dormant until triggered. A logic bomb is a specific example of an asynchronous attack. • A trigger activity may be a specific date and time, the launching of a specific program, or the processing of a specific type of activity. • Logic bombs do not self-replicate.

Hardware Attacks:

Common hardware attacks include:

- Manufacturing backdoors, for malware or other penetrative purposes; backdoors aren't limited to software and hardware, but they also affect embedded radio-frequency identification (RFID) chips and memory
- Eavesdropping by gaining access to protected memory without opening other hardware
- Inducing faults, causing the interruption of normal behavior
- Hardware modification tampering with invasive operations
- Backdoor creation; the presence of hidden methods for bypassing normal computer authentication systems
- Counterfeiting product assets that can produce extraordinary operations and those made to gain malicious access to systems.

Spectrum of attacks:

Types of spectrum

Anxiety, stress, and dissociation. Several types of spectrum are in use in these areas. **Obsessions and compulsions.** An obsessive–compulsive spectrum – this can include a Wide range of disorders.

General developmental disorders. An autistic spectrum – in its simplest form this Joins together autism and Asperger.

Psychosis. The schizophrenia spectrum or psychotic spectrum – there are numerouspsychotic spectrum disorders

Taxonomy of various attacks

The purpose of the Cyber Attacks section is to provide a general overview regarding cyber attacks, and to show some pragmatic ways to classify them and organize them via taxonomies.

Cyber attack: An offensive action by a malicious actor that is intended to undermine the functions of networked computers and their related resources, including unauthorized access, unapproved changes, and malicious destruction. Examples of cyber attacks include Distributed Denial of Service (DDoS) and Man-in-the- Middle (MITM) attacks.

The terms cyber attack, cyber threat, and cyber risk are interrelated as follows. A cyber attack is an offensive action, whereas a cyber threat is the possibility that a particular attack may occur, and the cyber risk associated with the subject threat estimates the probability of potential losses that may result.

For example, a Distributed Denial of Service (DDoS) cyber attack by a botnet is a cyber threat for many enterprises with online retail websites, where the associated cyber risk is a function of lost revenues due to website downtime and the probability that a DDoS cyber attack will occur.

Cyber Attack Malware Taxonomy

MALWARE TYPE	REQUIRES HOST FILE TO INFECT?	SELF-SPREADING?	APPEARS LEGITIMATE (HARMLESS)?	CAN CARRY HARMFUL PAYLOAD?	CAN COMMO WITH COMMAND & CONTROL SERVER?	CAN ATTACK OS KERNEL & FIRMWARE?
Virus	A	A	N/A	A	N/A	A
Worm	A	A	N/A	A	N/A	A
Trojan	A	A	A	A	N/A	A
Bots/Botnet	N/A	N/A	N/A	A	A	A
Spyware	A	A	N/A	A	A	A
Rootkit	N/A	N/A	N/A	A	N/A	A
Blended Threat	A	A	A	A	A	A

IP Spoofing:

IP spoofing is the creation of Internet Protocol (IP) packets which have a modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both. It is a technique often used by bad actors to invoke DDoS attacks against a target device or the surrounding infrastructure.

Sending and receiving IP packets is a primary way in which networked computers and other devices communicate, and constitutes the basis of the modern internet. All IPpackets contain a header which precedes the bodyof the packet and contains important routing information,

including the source address. In a normal packet, the source IP address is the address of the sender of the packet. If the packet has been spoofed, the source address will be forged.

IP Spoofing is analogous to an attacker sending a package to someone with the wrong return address listed. If the person receiving the package wants to stop the sender from sending packages, blocking all packages from the bogus address will do little good, as the return address is easily changed. Relatedly, if the receiver wants to respond to the return address, their response package will go somewhere other than to the real sender. The ability to spoof the addresses of packets is a core vulnerability exploited by many DDoS attacks.

DDoS attacks will often utilize spoofing with a goal of overwhelming a target with traffic while masking the identity of the malicious source, preventing mitigation efforts. If the source IP address is falsified and continuously randomized, blocking malicious requests becomes difficult. IP spoofing also makes it tough for law enforcement and cyber security teams to track down the perpetrator of the attack.

spoofing is also used to masquerade as another device so that responses are sent to that targeted device instead. Volumetric attacks such as NTP Amplification and DNS amplification make use of this vulnerability. The ability to modify the source IP is inherent to the design of TCP/IP, making it an ongoing security concern.

Tangential to DDoS attacks, spoofing can also be done with the aim of masquerading as another device in order to sidestep authentication and gain access to or "hijack" a user's session.

To protect against IP spoofing (packet filtering):

While IP spoofing can't be prevented, measures can be taken to stop spoofed packets from infiltrating a network. A very common defense against spoofing is ingress filtering, outlined in BCP38 (a Best Common Practice document). Ingress filtering is a form of packet filtering usually implemented on a network edge device which examines incoming IP packets and looks at their source headers. If the source headers on those packets don't match their origin or they otherwise look fishy, the packets are rejected. Some networks will also implement egress filtering, which looks at IP packets exiting the network, ensuring that those packets have legitimate source headers to prevent someone within the network from launching an outbound malicious attack using IP spoofing.

Methods of defense

The legal and ethical restrictions on computer-based crime. But unfortunately, computer crime is certain to continue for the foreseeable future. For this reason, we must look carefully at controls for preserving confidentiality, integrity, and availability. Sometimes these controls can prevent or mitigate attacks; other, less powerful methods can only inform us that security has

been compromised, by detecting a breach as it happens or after it occurs.

Harm occurs when a threat is realized against vulnerability. To protect against harm, then, we can neutralize the threat, close the vulnerability, or both. The possibility for harm to occur is called risk. We can deal with harm in several ways. We can seek to prevent it, by blocking the attack or closing the vulnerabilitydeter it, by making the attack harder but not impossible deflect it, by making another target more attractive (or this one less so)detect it, either as it happens or some time after the fact recover from its effects

Security models

The Cyber Security Model (CSM) is part of the Defence Cyber Protection Partnership (DCPP) which was set up by the Ministry of Defence (MOD) to manage and strengthen cyber security for the defence sector and its suppliers.

The model, which is a joint initiative between the MOD and industry, is in place to ensure that suppliers to the MOD are managing their cyber security risk appropriately, and that theyare capable of protecting the MOD's sensitive information.

The CSM is also the DCPP's response to the task of designing an appropriate and proportionate set of controls to build on the Government's Cyber Essentials scheme. Since January 2016, all suppliers dealing with contracts which include sensitive, MOD-identifiable information must be Cyber Essentials certified as a minimum.

However, some contracts carry an additional risk and require stricter security controls to be in place. The MOD felt that the Cyber Essentials scheme did not represent a broad enough degree of security because it only covered five major security controls and did not include wider aspects of cyber security such as governance and risk management, and this is whythe CSM was introduced.

Risk management

Cyber Security Risk Management

Risk management refers to the process of identifying, assessing, and controlling threats to a company's finances. These risks or threats could come from a number of sources including legal liabilities, strategic management mistakes, accidents, and natural disasters. As we move toward an increasingly digital way of life, cyber security introduces additional risks that have to be managed appropriately.

It's possible to invest in various types of insurance to protect physical assets from losses, but digital data isn't tangible – and therefore isn't covered under these kinds of policies.

Cyber security risk management relies on user education, strategy, and technology to protect an organization against attacks that could compromise systems, allow data to be

stolen, and ultimately damage the company's reputation. The rate of cyber attacks continues to grow both in terms of volume and severity. As such, businesses who want to protect themselves to the best of their ability must begin focusing efforts on cyber securityrisk management.

Cybersecurity Risk Management Process

You want to begin the process by starting with a cyber security framework that's been developed from each area of your business to determine what your desired risk posture should be.

It's a good idea to use technology that can help you find an app data across the organization. Once the data is mapped, you'll be able to make better decisions on how the data is governed and reduce your risk. For instance, even with training and strong security culture, it's possible for sensitive information to leave a company by accident. Leaving data stored in hidden rows across spreadsheets or included in notes within employee presentations or email threads leave your room for accidental data leakage. By scanning the company for sensitive data at rest and then removing any of that data stored where it does not belong, you greatly reduce the risk of accidental data loss.

Use the Community Maturity Model

Initial

This is the starting point for using a new or undocumented repeat process.Repeatable

At this stage, the process is documented well enough that repeating the same steps canbe attempted.

Defined

At this level, the process has been defined and is confirmed as a standard business process.

Managed

At this level, the process is quantitatively managed according to the agreed-upon metrics.

Optimizing

At the final stage, the process management process includes deliver it action to optimize and improve it.

Once you've determined the desired risk posture, take a look at your existing technology infrastructure to set the baseline for the current risk posture, then determine what must be done to move from the current state to the desired state.

As long as your organization is taking proactive steps to understand all the potential risks, you decrease the likelihood of running into a security incident that could hurt the

company.

A vital part of the risk management process is to conduct a risk and reward calculation. This helps prioritize security enhancements that will give you the greatest improvements at the lowest cost. Some companies may be comfortable with 99% of all security upgrades being made but others especially those in highly regulated industries, will want to be closer to 100%. Because of this, there should be incremental steps and goals such as a 5% Improvement achieved within 6 months, that can be measured to determine if the company is making progress toward its final goal.

That said, even small security vulnerabilities can lead to massive losses if systems are connected in a way that allows access to an unimportant area to bridge entry into systems that contain sensitive data.

The only way to ensure a system is fully secure is to make sure no one can access it – which isn't practical. The more you lock down a system, the harder it becomes for authorized personnel to conduct business as usual. If authorized users determine they cannot access the data they need to perform their jobs, they may look for workarounds that could easily result in compromised systems.

Mitigating Security Risks

So you will never be able to eliminate all cyber threats and security risks, there are a number of precautions you can take to mitigate risks when it comes to cybersecurity. Among these are the option to:

Limit devices with internet access

Limit the number of staff members with administrator credentials and control the rights for each administrator

Limit administrative rights

Use antivirus programs and endpoint security

Require users to implement two-factor authentication to gain access to certain files and systems

Install network access controls

Allow automatic updates and patches for operating

systems Place limits on older operating systems

Use firewalls

To take risk mitigation a step further, your organization may also want to consider advanced encryption, redaction, an element level security. Advanced encryption has to be implemented systematically and strategically to protect data from cybercriminals and insider threats. This includes standards-based cryptography, advanced key management, granular role-based access and separation of duties, and algorithms that drastically

decrease exposure.

Data encryption can help protect against outside breaches, but it doesn't do much to prevent internal data theft. Employees with access to sensitive data will have the credentials needed to decrypt it as part of their daily work, so organizations must also take action to prevent that data from being removed from the corporate system through flash drives and other removable media.

Redaction creates a balance between data protection and the ability to share it. With redaction, companies can share the information they need to share with minimal effort by hiding sensitive information such as names, social security numbers, addresses, and more.

Redaction is an important part of data security, but companies need to be able to do it at the property level based on employee roles. Companies also need to be able to implement custom and out of the box rules as necessary. With Purchase Control, user permission can be controlled at a highly granular level should go a long way toward preventing accounts payable fraud.

Cyber Threats:

Cyber Warfare: Cyber warfare refers to the use of digital attacks -- like computer viruses and hacking -- by one country to disrupt the vital computer systems of another, with the aim of creating damage, death and destruction. Future wars will see hackers using computer code to attack an enemy's infrastructure, fighting alongside troops using conventional weapons like guns and missiles.

Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.

Cyber Crime:

Cybercrime is criminal activitythat either targets or uses a computer, a computer network or a networked device. Cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out byindividuals or organizations.

Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.

Cyber Terrorism:

Cyber terrorism is the convergence of cyberspace and **terrorism**. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

Examples are hacking into computer systems, introducing viruses to vulnerable networks, web site defacing, Denial-of-service attacks, or terroristic threats made via electronic communication.

Cyber Espionage:

Cyber spying, or **cyber espionage**, is the act or practice of obtaining secrets and information without the permission and knowledge of the holder of the information from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet.

Security Policies:

Security policies are a formal set of rules which is issued by an organization to ensure that the user who are authorized to access company technology and information assets comply with rules and guidelines related to the security of information.

A security policy also considered to be a "living document" which means that the document is never finished, but it is continuously updated as requirements of the technology and employee changes.

We use security policies to manage our network security. Most types of security policies are automatically created during the installation. We can also customize policies to suit our specific environment.

Need of Security policies-

1) It increases efficiency.
2) It upholds discipline and accountability
3) It can make or break a business deal
4) It helps to educate employees on security literacy

There are some important cyber securitypolicies recommendations describe below-

Virus and Spyware Protection policy:

- It helps to detect threads in files, to detect applications that exhibits suspicious behavior.
- Removes, and repairs the side effects ofviruses and securityrisks byusing signatures.

Firewall Policy:

- It blocks the unauthorized users from accessing the systems and networks that connect to the Internet.
- It detects the attacks bycybercriminals and removes the unwanted sources of network traffic.

Intrusion Prevention policy:

- This policy automatically detects and blocks the network attacks and browser attacks.
- It also protects applications from vulnerabilities and checks the contents of one or more data packages and detects malware which is coming through legal ways.

Application and Device Control:

- This policy protects a system's resources from applications and manages the peripheraldevices that can attach to a system.
- The device control policy applies to both Windows and Mac computers whereas application control policy can be applied only to Windows clients.

UNIT- II
CYBERSPACE AND THE LAW & CYBER FORENSICS

CYBERSPACE

Cyberspace can be defined as an intricate environment that involves interactions between people, software, and services. It is maintained by the worldwide distribution of information and communication technologydevices and networks.

With the benefits carried by the technological advancements, the cyberspace today has become a common pool used by citizens, businesses, critical information infrastructure, military and governments in a fashion that makes it hard to induce clear boundaries among these different groups. The cyberspace is anticipated to become even more complex in the upcoming years, with the increase in networks and devices connected to it.

REGULATIONS

There are five predominant laws to cover when it comes to cybersecurity:

Information Technology Act, 2000 The Indian cyber laws are governed by the Information Technology Act, penned down back in 2000. The principal impetus of this Act is to offer reliable legal inclusiveness to eCommerce, facilitating registration of real-time records with the Government.

But with the cyber attackers getting sneakier, topped by the human tendency to misuse technology, a series of amendments followed.

The ITA, enacted by the Parliament of India, highlights the grievous punishments and penalties safeguarding the e-governance, e-banking, and e-commerce sectors. Now, the scope of ITA has been enhanced to encompass all the latest communication devices.

The IT Act is the salient one, guiding the entire Indian legislation to govern cybercrimes rigorously:

Section 43 - Applicable to people who damage the computer systems without permission fromthe owner. The owner can fully claim compensation for the entire damage in such cases.

Section 66 - Applicable in case a person is found to dishonestly or fraudulently committing any act referred to in section 43. The imprisonment term in such instances can mount up to three years or a fine of up to Rs. 5 lakh.

Section 66B - Incorporates the punishments for fraudulently receiving stolen communication devices or computers, which confirms a probable three years imprisonment. This term can also be topped byRs. 1 lakh fine, depending upon the severity.

Section 66C - This section scrutinizes the identity thefts related to imposter digital signatures, hacking passwords, or other distinctive identification features. If proven guilty, imprisonment of three years might also be backed by Rs.1 lakh fine.

Section 66 D - This section was inserted on-demand, focusing on punishing cheaters doing impersonation using computer resources.

Indian Penal Code (IPC) 1980

Identity thefts and associated cyber frauds are embodied in the Indian Penal Code (IPC), 1860 - invoked along with the Information Technology Act of 2000.

The primary relevant section ofthe IPC covers cyber frauds:

Forgery(Section 464)

Forgerypre-planned for cheating (Section 468)

False documentation (Section 465)

Presenting a forged document as genuine (Section 471)

Reputation damage (Section 469)

Companies Act of2013

The corporate stakeholders refer to the Companies Act of 2013 as the legal obligation necessary for the refinement of daily operations. The directives of this Act cements all the required techno-legal compliances, putting the less compliant companies in a legal fix.

The Companies Act 2013 vested powers in the hands of the SFIO (Serious Frauds Investigation Office) to prosecute Indian companies and their directors. Also, post the notification of the Companies Inspection, Investment, and Inquiry Rules, 2014, SFIOs has become even more proactive and stern in this regard.

The legislature ensured that all the regulatory compliances are well-covered, including cyber forensics, e-discovery, and cybersecurity diligence. The Companies (Management and Administration) Rules, 2014 prescribes strict guidelines confirming the cybersecurity obligations and responsibilities upon the company directors and leaders.

NIST Compliance

The Cybersecurity Framework (NCFS), authorized by the National Institute of Standards and Technology (NIST), offers a harmonized approach to cybersecurity as the most reliable global certifying body.

NIST Cybersecurity Framework encompasses all required guidelines, standards, and best practices to manage the cyber-related risks responsibly. This framework is prioritized on flexibility and cost-effectiveness.

It promotes the resilience and protection of critical infrastructure by: Allowing better interpretation, management, and reduction of cybersecurity risks – to mitigate data loss, data misuse, and the subsequent restoration costs Determining the most important activities and critical operations - to focus on securing them Demonstrates the trust-worthiness of organizations who secure critical assets Helps to prioritize investments to maximize the cybersecurity ROI Addresses regulatory and contractual obligations Supports the wider information security program By combining the NIST CSF framework with ISO/IEC 27001 - cybersecurity risk management becomes simplified. It also makes communication easier

throughout the organization and across the supply chains via a common cybersecurity directive laid by NIST.

Final Thoughts As human dependence on technology intensifies, cyber laws in India and across the globe need constant up-gradation and refinements. The pandemic has also pushed much of the workforce into a remote working module increasing the need for app security. Lawmakers have to go the extra mile to stay ahead of the impostors, in order to block them at their advent.

Cybercrimes can be controlled but it needs collaborative efforts of the lawmakers, the Internet or Network providers, the intercessors like banks and shopping sites, and, most importantly, the users. Only the prudent efforts of these stakeholders, ensuring their confinement to the law of the cyberland - can bring about online safety and resilience.

ROLE OF INTERNATIONAL LAWS

In various countries, areas of the computing and communication industries are regulated by governmental bodies There are specific rules on the uses to which computers and computer networks may be put, in particular there are rules on unauthorized access, data privacy and spamming There are also limits on the use of encryption and of equipment which may be used to defeat copy protection schemes There are laws governing trade on the Internet, taxation, consumer protection, and advertising There are laws on censorship versus freedom of expression, rules on public access to government information, and individual access to information held on them by private bodies Some states limit access to the Internet, by law as well as by technical means.

INTERNATIONAL LAW FOR CYBER CRIME

Cybercrime is "international" that there are 'no cyber-borders between countries' The complexity in types and forms of cybercrime increases the difficulty to fight back fighting cybercrime calls for international cooperation Various organizations and governments have already made joint efforts in establishing global standards of legislation and law enforcement both on a regional and on an international scale

THE INDIAN CYBERSPACE

Indian cyberspace was born in 1975 with the establishment of National Informatics Centre (NIC) with an aim to provide govt with IT solutions. Three networks (NWs) were set up between 1986 and 1988 to connect various agencies of govt. These NWs were, INDONET which connected the IBM mainframe installations that made up India's computer infrastructure, NICNET (the NIC NW) a nationwide very small aperture terminal (VSAT) NW for public sector organisations as well as to connect the central govt with the state govts and district administrations, the third NW setup was ERNET (the Education and Research Network), to serve the academic and research communities.

New Internet Policy of 1998 paved the way for services from multiple Internet service providers (ISPs) and gave boost to the Internet user base grow from 1.4 million in 1999 to over 150 million by Dec 2012. Exponential growth rate is attributed to increasing Internet

access through mobile phones and tablets. Govt is making a determined push to increase broadband penetration from its present level of about 6%1. The target for broadband is 160 million households by2016 under the National Broadband Plan.

NATIONAL CYBER SECURITY POLICY

National Cyber Security Policy is a policy framework by Department of Electronics and Information Technology. It aims at protecting the public and private infrastructure from cyberattacks. The policy also intends to safeguard "information, such as personal information (of web users), financial and banking information and sovereign data". This was particularly relevant in the wake of US National Security Agency (NSA) leaks that suggested the US government agencies are spying on Indian users, who have no legal or technical safeguards against it. Ministry of Communications and Information Technology (India) defines Cyberspace as a complex environment consisting of interactions between people, software services supported by worldwide distribution of information and communication technology.

VISION

To build a secure and resilient cyberspace for citizens, business, and government and also to protect anyone from intervening in user's privacy.

MISSION

To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threat, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology, and cooperation.

OBJECTIVE

Ministry of Communications and Information Technology (India) define objectives as follows:

- To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.
- To create an assurance framework for the design of security policies and promotion and enabling actions for compliance to global security standards and best practices by wayof conformityassessment (Product, process, technology & people).
- To strengthen the Regulatory Framework for ensuring a SECURE CYBERSPACE ECOSYSTEM.
- To enhance and create National and Sectoral level 24X7 mechanism for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective response and recoveryactions.

INTRODUCTION: CYBER FORENSICS

CYBER FORENSICS:

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence.

Forensic examiners typically analyze data from personal computers, laptops, personal digital assistants, cell phones, servers, tapes, and any other type of media. This process can involve anything from breaking encryption, to executing search warrants with a law enforcement team, to recovering and analyzing files from hard drives that will be critical evidence in the most serious civil and criminal cases.

The forensic examination of computers, and data storage media, is a complicated and highly specialized process. The results of forensic examinations are compiled and included in reports. In many cases, examiners testify to their findings, where their skills and abilities are put to ultimate scrutiny.

DIGITAL FORENSICS:

Digital Forensics is defined as the process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law. It is a science of finding evidence from digital media like a computer, mobile phone, server, or network. It provides the forensic team with the best techniques and tools to solve complicated digital-related cases.

Digital Forensics helps the forensic team to analyzes, inspect, identifies, and preserve the digital evidence residing on various types of electronic devices.

Digital forensic science is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrime.

THE NEED FOR COMPUTER FORENSICS

Computer forensics is also important because it can save your organization money From a technical standpoint, the main goal of computer forensics is to identify, collect, preserve, and analyze data in a way that preserves the integrity of the evidence collected so it can be used effectively in a legal case.

CYBER FORENSICS AND DIGITAL EVIDENCE:

Digital evidence is information stored or transmitted in binary form that may be relied on in court. It can be found on a computer hard drive, a mobile phone, among other places. Digital evidence is commonly associated with electronic crime, or e-crime, such as child pornography or credit card fraud. However, digital evidence is now used to prosecute all types of crimes, not just e-crime. For example, suspects' e-mail or mobile phone files might contain critical evidence regarding their intent, their whereabouts at the time of a crime and their relationship with other suspects. In 2005, for example, a floppy disk led investigators to the BTK serial killer who had eluded police capture since 1974 and claimed the lives of at least 10 victims.

In an effort to fight e-crime and to collect relevant digital evidence for all crimes, law enforcement agencies are incorporating the collection and analysis of digital evidence, also known as computer forensics, into their infrastructure. Law enforcement agencies are challenged by the need to train officers to collect digital evidence and keep up with rapidly evolving technologies such as computer operating systems.

UNIT- III

CYBERCRIMES: MOBILE AND WIRELESS

INTRODUCTION: Why should *mobile devices* be protected? Every day, *mobile devices* are lost, stolen, and infected. *Mobile devices* can store important business and personal *information,* and are often be used to access Universitysystems, email, banking

Proliferation of mobile and wireless devices:

- people hunched over their smartphones or tablets in cafes, airports, supermarkets and even at bus stops, seeminglyoblivious to anything or anyone around them.
- They play games, download email, go shopping or check their bank balances on the go.

They might even access corporate networks and pull up a document or two on their mobile gadgets

Today, incredible advances are being made for mobile devices. The trend is for smaller devices and more processing power. A few years ago, the choice was between a wireless phone and a simple PDA. Now the buyers have a choice between high-end PDAs with integrated wireless modems and small phones with wireless Web-browsing capabilities. A long list of options is available to the mobile users. A simple hand-held mobile device provides enough computing power to run small applications, play games and music, and make voice calls. A key driver for the growth of mobile technology is the rapid growth of business solutions into hand-held devices.

As the term "mobile device" includes many products. We first provide a clear distinction among the key terms: mobile computing, wireless computing and hand-held devices. Figure below helps us understand how these terms are related. Let us understand the concept of mobile computing and the various types of devices.

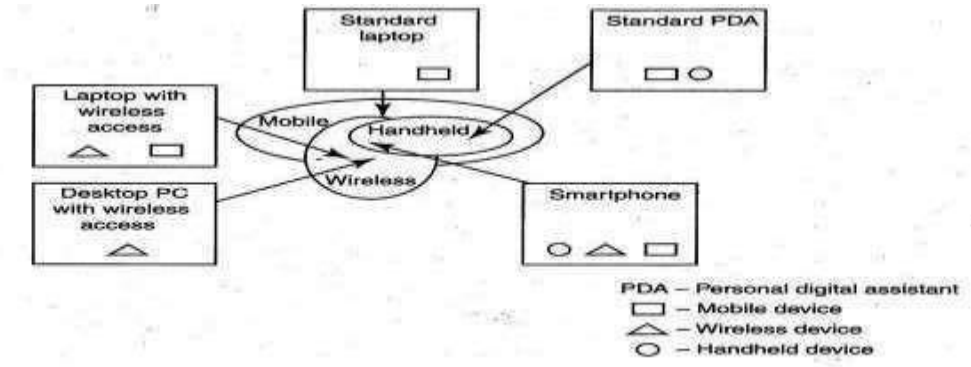


Figure : Mobile, Wireless and hand-held Devices

Mobile computing is "taking a computer and all necessary files and software out into the field." Many types of mobile computers have been introduced since 1990s. They are as follows:

1. Portable computer: It is a general-purpose computer that can be easily moved from one place to another, but cannot be used while in transit, usually because it requires some "setting-up" and an AC power source.

2. Tablet PC: It lacks a keyboard, is shaped like a slate or a paper notebook and has features of a touchscreen with a stylus and handwriting recognition software. Tablets may not be best suited for applications requiring a physical keyboard for typing, but are otherwise capable of carrying out most tasks that an ordinary laptop would be able to perform.

3. Internet tablet: It is the Internet appliance in tablet form. Unlike a Tablet PC, the Internet tablet does not have much computing power and its applications suite is limited. Also it cannot replace a general-purpose computer. The Internet tablets typically feature an MP3 and video player, a Web browser, a chat application and a picture viewer.

4. Personal digital assistant (PDA): It is a small, usually pocket-sized, computer with limited functionality. It is intended to supplement and synchronize with a desktop computer, giving access to contacts, address book, notes, E-Mail and other features.

5. Ultramobile (PC): It is a full-featured, PDA-sized computer running a general-purpose operating system (OS).

6. Smartphone: It is a PDA with an integrated cell phone functionality. Current Smartphones have a wide range of features and installable applications.

7. Carputer: It is a computing device installed in an automobile. It operates as a wireless computer, sound system, global positioning system (GPS) and DVD player. It also contains word processing software and is Bluetooth compatible.

8. Fly Fusion Pentop computer: It is a computing device with the size and shape of a pen. It functions as a writing utensil, MP3 player, language translator, digital storage device and calculator.

Trends in Mobility:

Mobile computing is moving into a new era, third generation (3G), which promises greater variety in applications and have highly improved usability as well as speedier networking. "iPhone" from Apple and Google-led "Android" phones are the best examples of this trend and there are plenty of other developments that point in this direction. This smart mobile technology is rapidly gaining popularity and the attackers (hackers and crackers) are among its biggest fans.

It is worth noting the trends in mobile computing; this will help readers to readers to realize the seriousness of cybersecurity issues in the mobile computing domain. Figure below shows the different types of mobility and their implications.

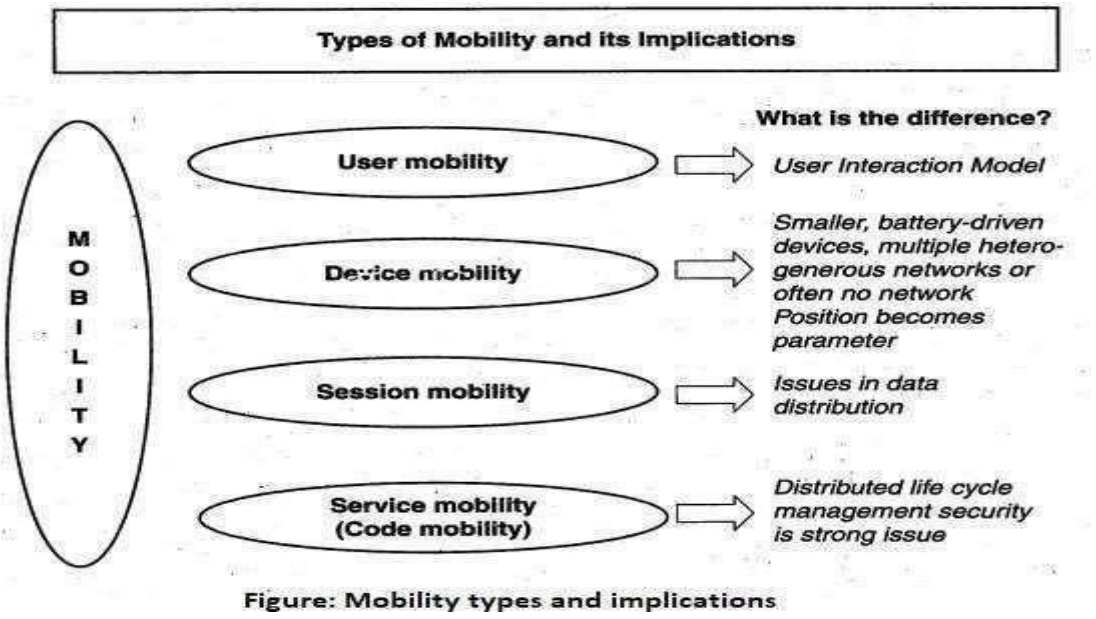


Figure: Mobility types and implications

The new technology 3G networks are not entirely built with IP data security. Moreover, IP data world when compared to voice-centric security threats is new to mobile operators. There are numerous attacks that can be committed against mobile networks and they can originate from two primary vectors. One is from outside the mobile network - that is, public Internet, private networks and other operator's networks - and the other is within the mobile networks-that is, devices such as data-capable handsets and Smartphones, notebook computers or even desktop computers connected to the 3G network.

Popular types ofattacks against 3G mobile networks are as follows:

1. Malwares, viruses and worms: Although many users are still in the transient process of switching from 2G,2.5G2G,2.5G to 3G,3G, it is a growing need to educate the community people and provide awareness of such threats that exist while using mobile devices. Here are few examples of malware(s) specific to mobile devices:

- ***Skull Trojan:*** Itargets Series 60 phones equipped with the Symbian mobile OS.
- ***Cabir Worm:*** It is the first dedicated mobile-phone worm infects phones running on Symbian OS and scans other mobile devices to send a copy of itself to the first vulnerable phone it finds through Bluetooth Wireless technology. The worst thing about this worm is that the source code for the Cabir-H and Cabir-I viruses is available online.
- ***Mosquito Trojan:*** It affects the Series 60 Smartphones and is a cracked version of "Mosquitos" mobile phone game.
- ***Brador Trojan:*** It affects the Windows CE OS by creating a svchost. exe file in the Windows start-up folder which allows full control of the device. This executable file is conductive to traditional worm propagation vector such as E-Mail file attachments.
- ***Lasco Worm:*** It was released first in 2005 to target PDAs and mobile phones running the Symbian OS. Lasco is based on Cabir's source code and replicates over Bluetooth connection.

2. Denial-of-service (DoS): The main objective behind this attack is to make the system unavailable to the intended users. Virus attacks can be used to damage the system to make the system unavailable. Presently, one of the most common cyber security threats to wired Internet service providers (iSPs) is a distributed denial-of-service (DDos) attack .DDoS

attacks are used to flood the target system with the data so that the response from the target system is either slowed or stopped.

3. Overbilling attack: Overbilling involves an attacker hijacking a subscriber's IP address and then using it (i.e., the connection) to initiate downloads that are not "Free downloads" or simply use it for his/her own purposes. In either case, the legitimate user is charged for the activitywhich the user did not conduct or authorize to conduct.

4. Spoofed policy development process (PDP): These of attacks exploit the vulnerabilities in the GTP [General Packet Radio Service (GPRS) Tunneling Protocol].

5. Signaling-level attacks: The Session Initiation Protocol (SIP) is a signaling protocol used in IP multimedia subsystem (IMS) networks to provide Voice Over Internet Protocol (VoIP) services. There are several vulnerabilities with SIP-based VolP systems.

Credit Card Frauds in Mobile and Wireless Computing Era:

These are new trends in cybercrime that are coming up with mobile computing - mobile commerce (M-Commerce) and mobile banking (M-Banking). Credit card frauds are now becoming commonplace given the ever-increasing power and the ever-reducing prices of the mobile hand-held devices, factors that result in easy availability of these gadgets to almost anyone. Today belongs to "mobile compüting," that is, anywhere anytime computing. The developments in wireless technology have fuelled this new mode of working for white collar workers. This is true for credit card processing too; wireless credit card processing is a relatively new service that will allow a person to process credit cards electronically, virtually anywhere. Wireless credit card processing is a very desirable system, because it allows businesses to process transactions from mobile locations quickly, efficiently and professionally. It is most often used by businesses that operate mainly in a mobile environment

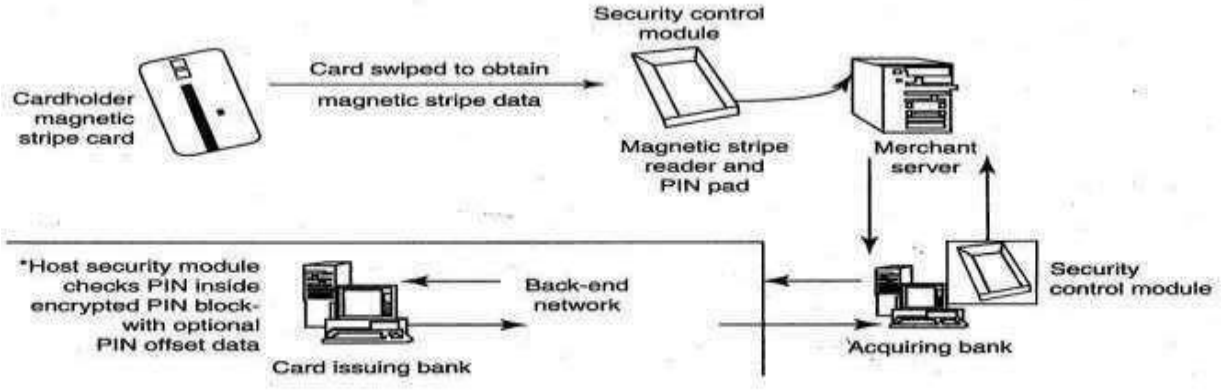


Figure : Online environment for credit card transactions

There is a system available from an Australian company "Alacrity" called closed-loop environment for for wireless (CLEW). Figure above shows the flow of events with CLEW which is a registered trademark of Alacrity used here only to demonstrate the flow in this environment.

As shown in Figure, the basic flow is as follows:

1. Merchant sends a transaction to bank
2. The bank transmits the request to the authorized cardholder
3. The cardholder approves or rejects (password protected)

4. The bank/merchant is notified
5. The credit card transaction is completed.

Security Challenges Posed by Mobile Devices:

Mobility brings two main challenges to cybersecurity: first, on the hand-held devices, information is being taken outside the physically controlled environment and second remote access back to the protected environment is being granted. Perceptions of the organizations to these cybersecurity challenges are important in devising appropriate security operating procedure. When people are asked about important in managing a diverse range of mobile devices, theyseem to be thinking of the ones shown in below figure.

As the number of mobile device users increases, two challenges are presented: one at the device level called "micro challenges" and another at the organizational level called "macro-challenges."

Some well-known technical challenges in mobile security are: managing the registry settings and configurations, authentication service security, cryptography security, Lightweight Directory Access Protocol (LDAP) security, remote access server (RAS) security, media player control security, networking application program interface (API), securityetc.

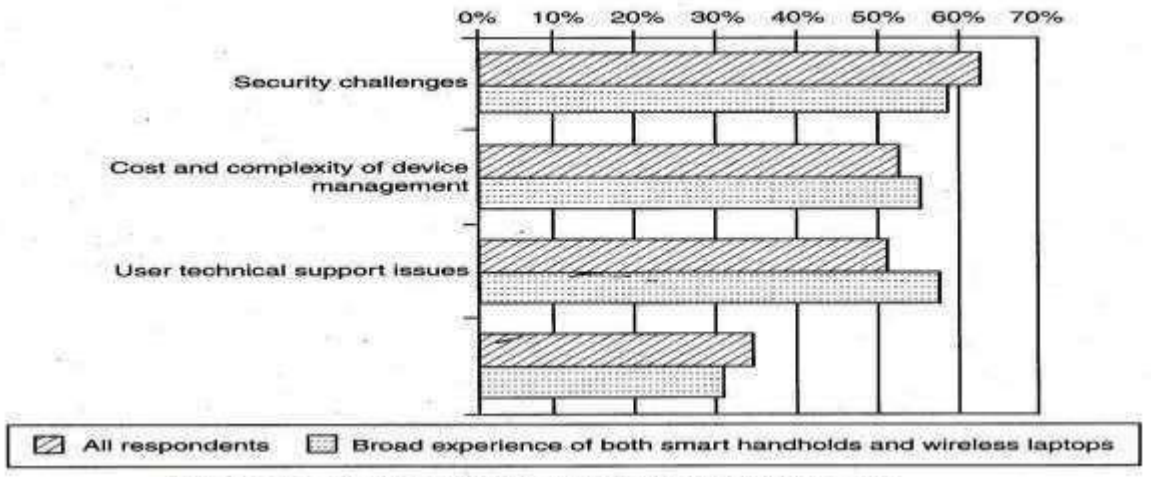


Figure: Important issues for managing mobile devices

Registry Settings for Mobile Devices:

Let us understand the issue of registry settings on mobile devices through an example: Microsoft Activesync is meant for synchronization with Windows-powered personal computers (PCs) and Microsoft Outlook. ActiveSync acts as the "gateway between Windows-powered PC and Windows mobile-powered device, enabling the transfer of applications such as Outlook information, Microsoft Office documents, pictures, music, videos and applications from a user's desktop to his/her device.

In addition to synchronizing with a PC, ActiveSync can synchronize directly with the Microsoft exchange server so that the users can keep their E-Mails, calendar, notes and contacts updated wirelessly when they are away from their PCs. In this context, registry setting becomes an important issue given the ease with which various applications allow a free flow of information.

Authentication Service Security:

There are two components of security in mobile computing: security of devices and security in networks. A secure network access involves authentication between the device and the base stations or Web servers. This is to ensure that only authenticated devices can be

connected to the network for obtaining the requested services. No Malicious Code can impersonate the service provider to trick the device into doing something it does not mean to. Thus, the networks also playa crucial role in securityof mobile devices.
Some eminent kinds of attacks to which mobile devices are subjected to are: push attacks, pull attacks and crash attacks.
Authentication services security is important given the typical attacks on mobile devices through wireless networks: Dos attacks, traffic analysis, eavesdropping, man-in-the-middle attacks and session hijacking. Security measures in this scenario come from Wireless Application Protocols (WAPs), use of VPNs, media access control (MAC) address filtering and development in 802.xx standards.

Attacks on Mobile-Cell Phones:

- **Mobile Phone Theft:**

Mobile phones have become an integral part of everbody's life and the mobile phone has transformed from being a luxury to a bare necessity. Increase in the purchasing power and availability of numerous low cost handsets have also lead to an increase in mobile phone users. Theft of mobile phones has risen dramatically over the past few years. Since huge section of working population in India use public transport, major locations where theft occurs are bus stops, railway stations and traffic signals.
The following factors contribute for outbreaks onmobile devices:

1. Enough target terminals: The first Palm OS virus was seen after the number of Palm OS devices reached 15 million. The first instance of a mobile virus was observed during June 2004 when it was discovered that an organization "Ojam" had engineered an antipiracy Trojan virus in older versions of their mobile phone game known as Mosquito. This virus sent SMS text messages to the organization without the users' knowledge.

2. Enough functionality: Mobile devices are increasingly being equipped with office functionality and already carry critical data and applications, which are often protected insufficiently or not at all. The expanded functionality also increases the probability of malware.

3. Enough connectivity: Smartphones offer multiple communication options, such as SMS, MMS, synchronization, Bluetooth, infrared (IR) and WLAN connections. Therefore, unfortunately, the increased amount of freedom also offers more choices for virus writers.

- Mobile - Viruses
- **Concept of Mishing**
- **Concept of Vishing**
- **Concept of Smishing**
- **Hacking - Bluetooth**

Mobile Devices: Security Implications for Organizations

Managing diversity and proliferation of hand-held devices

We have talked about the micro issues of purely technical nature in mobile device security. Given the threats to information systems through usage of mobile devices, the organizations need to establish security practices at a level appropriate to their securityobjectives, subject to legaland other externalconstraints.

Unconventional/stealth storage devices

We would like to emphasize upon widening the spectrum of mobile devices and focuson secondary storage devices, such as compact disks (CDs) and Universal Serial Bus (USB) drives (also called zip drive, memorysticks) used by employees.

As the technology is advancing, the devices continue to decrease in size and emerge in new shapes and sizes – unconventional/stealth storage devices available nowadays are difficult to detect and have become a prime challenge for organizational security.

The features of the software allows system administrator to:

Monitor which users or groups can access USB Ports,

Wi-Fi and Bluetooth adapters, CD read-only memories (CD-ROMs) and other removable devices.

Control the access to devices depending on the time of the dayand day of the week.

Createthe white list of USB devices whichallows you to authorize onlyspecific devices that will not be locked regardless of anyother settings.

Set devices in read-only mode.

Protect disks from accidental or intentional formatting.

Threats through lost and stolen devices

This is a new emerging issue for cyber security. Often mobile hand-held devices are lost while people are on the move. Lost mobile devices are becoming even a larger security risk to corporations.

Organizational Measures for Handling Mobile

A report based on a survey of London's 24,000 licensed cab drivers quotes that 2,900 laptops, 1,300 PDAs and over 62,000 mobile phones were left in London in cabs in the year 2001 over the last 6-month period.

Protecting data on lost devices

Readers can appreciate the importance of data protection especially when it resides ona mobile hand-held device. At an individual level, employees need to worryabout this.

Organizational security Policies and Measures in Mobile Computing Era:

Proliferation of hand-held devices used makes the cybersecurity issue graver than what we would tend to think. People have grown so used to their hand-helds they are treating them like wallets! For example, people are storing more types of confidential information on mobile computing devices than their employers or they themselves know; they listen to music using their-hand-held devices. One should think about not to keep credit card and bank account numbers, passwords, confidential E-Mails and strategic information about organization, merger or takeover plans and also other valuable information that could impact stock values in the mobile devices. Imagine the business impact if an employee's USB, pluggable drive or laptop was lost or stolen, revealing sensitive customer data such as credit reports, social security numbers (SSNs) and contact information.

Operating Guidelines for Implementing Mobile Device Security Policies

In situations such as those described above, the ideal solution would be to prohibit all confidential data from being stored on mobile devices, but this may not always be practical. Organizations can, however, reduce the risk that confidential information will be accessed from lost or stolen mobile devices through the following steps:

1. Determine whether the employees in the organization need to use mobile computing devices at all, based on their risks and benefits within the organization, industry and regulatoryenvironment.
2. Implement additional security technologies, as appropriate to fit both the organization and the types of devices used. Most (and perhaps all) mobile computing devices will need to have their native security augmented with such tools as strong encryption, device passwords and physical locks. Biometrics techniques can be used for authentication and encryption and have great potential to eliminate the challenges associated with passwords.
3. Standardize the mobile computing devices and the associated security tools being used with them. As a matter of fundamental principle, security deteriorates quickly as the tools and devices used become increasingly disparate.
4. Develop a specific framework for using mobile computing devices, including guidelines for data syncing, the use of firewalls and anti-malware software and the types of information that can be stored on them.
5. Centralize management of your mobile computing devices. Maintain an inventory so that you know who is using what kinds of devices.,
6. Establish patching procedures for software on mobile devices. This can often be simplified by integrating patching with syncing or patch management with the centralized
7. Provide education and awareness training to personnel using mobile devices. People cannot be expected to appropriately secure their information if they have not been told how.

Organizational Policies for the Use of Mobile Hand-Held Devices

There are many ways to handle the matter of creating policy for mobile devices. One way is creating distinct mobile computing policy. Another way is including such devices existing policy. There are also approaches in between where mobile devices fall under both existing policies and a new one.In the hybrid approach, a new policy is created to address the specific needs of the mobile devices but more general usage issues fall under general IT policies. As a

part of this approach, the "acceptable use" policy for other technologies is extended to the mobile devices.

Companies new to mobile devices may adopt an umbrella mobile policy but they find over time the the they will need to modify their policies to match the challenges posed by different kinds of mobile hand-held devices. For example, wireless devices pose different challenges than non-wireless Also, employees who use mobile devices more than 20%% of the time will have different requirements than less-frequent users. It may happen that over time, companies may need to create separate policies for the mobile devices on the basis of whether they connect wirelessly and with distinctions for devices that connect to WANs and LANs .

Concept of Laptops:

As the price of computing technology is steadily decreasing, usage of devices such as the laptops is becoming more common. Although laptops, like other mobile devices, enhance the business functions owing to their mobile access to information anytime and anywhere, they also pose a large threat as they are portable Wireless capability in these devices has also raised cyber security concerns owing to the information being transmitted over other, which makes it hard to detect.

The thefts of laptops have always been a major issue, according to the cybersecurity industry and insurance company statistics. Cybercriminals are targeting laptops that are expensive, to enable them to fetch a quick profit in the black market. Very few laptop. thieves. are actually interested in the information that is contained in the laptop. Most laptops contain personal and corporate information that could be sensitive..

Physical Security Countermeasures

Organizations are heavily dependent upon a mobile workforce with access to information, no matter where they travel. However, this mobility is putting organizations at risk of having a data breach if a laptop containing sensitive information is lost or stolen. Hence, physical security countermeasures are becoming very vital to protect the information on the employees laptops and to reduce the likelihood that employees will lose laptops.

1. Cables and hardwired locks: The most cost-efficient and ideal solution to safeguard any mobile device is securing with cables and locks, specially designed for laptops. Kensington cables are one of the most popular brands in laptop security cable. These cables are made of aircraft-grade steel and Kevlar brand fiber, thus making these cables 40%% stronger than any other conventional security cables. One end of the security cable is fit into the universal security slot of the laptop and the other end is locked around any fixed furniture or item, thus making a loop. These cables come with a variety of options such as number locks, key locks and alarms.

2. Laptop safes: Safes made of polycarbonate - the same material that is used in bulletproof windows, police riot shields and bank security screens-can be used to carry and safeguard the laptops. The advantage of safes over security cables is that they protect the whole laptop and its devices such as CD-ROM bays, PCMCIA cards and HDD bays which can be easily removed in the case of laptops protected bysecurity cables.

3. Motion sensors and alarms: Even though alarms and motion sensors are annoying owing to their false alarms and loud sound level, these devices are very efficient in securing laptops. Once these devices are activated, they can be used to track missing laptops in crowded places. Also owing to their loud nature, they help in deterring thieves. Modern systems for laptops are designed wherein the alarm device attached to the laptop transmits radio signals to a certain range around the laptop.

4. Warning labels and stamps: Warning labels containing tracking information and identification details can be fixed onto the laptop to deter aspiring thieves. These labels

cannot be removed easily and are a low-cost solution to a laptop theft. These labels have an identification number that is stored in a universal database for verification, which, in turn makes the resale of stolen laptops a difficult process. Such labels are highly recommended for the laptops issued to top executives and/or keyemployees of the organizations.

5. Other measures for protecting laptops are as follows:

- Engraving the laptop with personal details
- Keeping the laptop close to oneself wherever possible
- Carrying the laptop in a different and unobvious bag making it unobvious to potential thieves
- Creating the awareness among the employees to understand the responsibility of carrying a laptop and also about the sensitivity of the information contained in the laptop
- Making a copy of the purchase receipt, laptop serial number and the description of the laptop
- Installing encryption software to protect information stored on the laptop
- Using personal firewall software to block unwanted access and intrusion
- Updating the antivirus software regularly
- Tight office security using securityguards and securing the laptop by locking it down in lockers when not in use
- Never leaving the laptop unattended in public places such as the car, parking lot, conventions, conferences and the airport until it is fitted with an antitheft device;
- Disabling IR ports and wireless cards and removing PCMCIA cards when not in use.

Information systems security also contains logical access controls. This is because, information, be it corporate or private, needs high security as it is the most important asset of an organization or an individual. A few logical or access controls are as follows:

1. Protecting from malicious programs/attackers/social engineering.
2. Avoiding weak passwords/ access.
3. Monitoring application securityand scanning for vulnerabilities.
4. Ensuring that unencrypted data/unprotected file systems do not pose threats.
5. Proper handing of removable drives/storage mediums /unnecessaryports.
6. Password protection through appropriate passwords rules and use of strong passwords.
7. Locking down unwanted ports/devices.
8. Regularly installing securitypatches and updates.
9. Installing antivirus software/firewalls / intrusion detection system (IDSs).
10. Encrypting critical file systems.

UNIT-IV
Cybersecurity: Organizational Implications

Introduction:

In the global environment with continuous network connectivity, the possibilities for cyberattacks can emanate from sources that are local, remote, domestic or foreign. They could be launched by an individual or a group. They could be casual probes from hackers using personal computers (PCs) in their homes, hand-held devices or intense scans from criminal groups.
Most information the organization collects about an individual is likely to come under "PI" category if it can be attributed to an individual. For an example, PI is an individual's first name or first initial and last name in combination with any of the following data:

1. Social securitynumber (SSN)/social insurance number.
2. Driver's license number or identification card number.
3. Bank account number, credit or debit card number with personal identification number such as an access code, security codes or password that would permit access to an individual's financial account.
4. Home address or E-Mail address.
5. Medical or health information.

An insider threat is defined as "the misuse or destruction of sensitive or confidential information, as well as IT equipment that houses this data by employees, contractors and other 'trusted' individuals."

Insider threats are caused by human actions such as mistakes, negligence, reckless behavior, theft, fraud and even sabotage. There are three types of "insiders" such as:

1. A malicious insider is motivated to adversely impact an organization through a range of actions that compromise information confidentiality, integrityand/or availability.
2. A careless insider can bring about a data compromise not by any bad intention but simply by being careless due to an accident, mistake or plain negligence.
3. A tricked insider is a person who is "tricked" into or led to providing sensitive or private company data by people who are not truthful about their identity or purpose via "pretexting" (known as social engineering)

Insider Attack Example 1: Heartland Payment System Fraud

- A case in point is the infamous "Heartland Payment System Fraud" that was uncovered in January2010.
- In this case, the concerned organization suffered a serious blow through nearly 100 million credit cards compromised from at least 650 financial services companies.
- When a card is used to make a purchase, the card information is transmitted through a payment network.
- A piece of malicious software (keystroke logger) planted on the company's payment processing network; recorded payment card data as it was being sent for processing to Heartland by thousands of the company's retail clients.
- Digital information within the magnetic stripe on the back of credit/debit cards was copied by **keylogger.**
- Criminal created counterfeit credit cards.

Insider Attack Example 2: Blue Shield Blue Cross (BCBS)

- Yet another incidence is the Blue Cross Blue Shield (BCBS) Data Breach in October 2009 the theft of 57 hard drives from a BlueCross BlueShield of Tennessee training facility puts the private information of approximately 500,000 customers at risk in at least 32 states.
- The hard drives containing 1.3 million audio files and 300,000 video files related to coordination of care and eligibility telephone calls from providers and members were reportedly stolen from a leased office.
    1. Physical security is very important.
    2. Insider threats cannot be ignored.

Privacy has following four key dimensions:

1. **Informational/data privacy:** It is about data protection, and the user's rights to determine how, when and to what extent information about them is communicated to other parties.
2. **Personal privacy:** It is about content filtering and other mechanisms to ensure that the end-users are not exposed to whatever violates their moral senses.
3. **Communication privacy:** This is as in networks, where encryption of data being transmitted is important.
4. **Territorial privacy:** It is about protecting user's property.
   For example, the user devices from being invaded byundesired content such as SMS or E-Mail/Spam messages.

The keychallenges from emerging new information threats to organizations are as follows:

1. **Industrial espionage:** There are several tools available for web administrators to monitor and track the various pages and objects that are accessed on their website.
2. **IP-based blocking:** This process is often used for blocking the access of specific IP addresses and/or domain names.
3. **IP-based "cloaking":** Businesses are global in nature and economies are interconnected. There are websites that change their online content depending on a user's IP address or user's geographic location.
4. **Cyberterrorism:** "Cyberterrorism" refers to the direct intervention of a threat source toward your organization's website.
5. **Confidential information leakage:** "Insider attacks" are the worst ones. Typically, an organization is protected from external threats by your firewall and antivirus solution.

Cost of Cybercrimes and IPR Issues: Lessons for Organizations

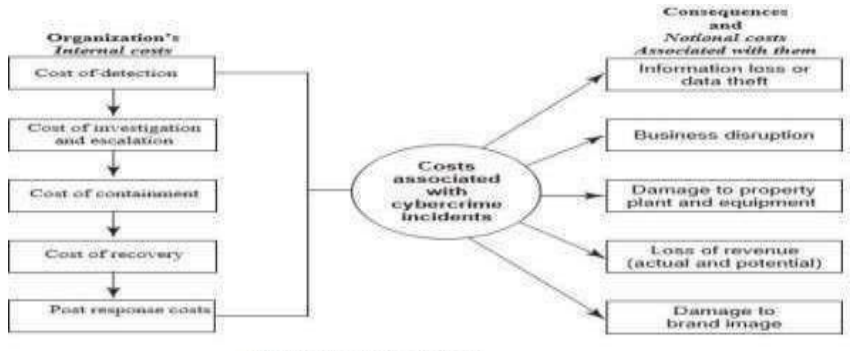


Fig: Cost of cybercrimes.

When a cybercrime incidence occurs, there are a number of internal costs associated with it for organizations and there are organizational impacts as well.

- **Organizations have Internal Costs Associated with Cyber security Incidents**
  The internal costs typically involve people costs, overhead costs and productivity losses. The internal costs, in order from largest to the lowest and that has been supported by the benchmark study mentioned:
    1. Detection costs.(25%)
    2. Recovery costs.(21%)
    3. Post response costs.(19%)
    4. Investigation costs.(14%)
    5. Costs of escalation and incident management.(12%)
    6. Cost of containment.(9%)
- The consequences of cybercrimes and their associated costs, mentioned
    1. Information loss/data theft.(42%)
    2. Business disruption.(22%)
    3. Damages to equipment, plant and property.(13%)
    4. Loss of revenue and brand tarnishing.(13%)
    5. Other costs.(10%)
- The impact on organizations by various cyber crimes
    1. Virus,worms and Trojans-100%
    2. Malwares-80%
    3. Botnets-73%
    4. Web based attacks-53%
    5. Phishing and Social engineering-47%
    6. Stolen devices-36%
    7. Malicious insiders-29%
    8. Malicious code-27%
- Average days taken to resolve cyber Attacks
    1. Attacks by Malicious insiders-42 days
    2. Malicious code-39 days
    3. Web based attacks-19 days
    4. Data lost due to stolen devices-10 days
    5. Phishing and social engineering attacks-9 days
    6. Virus,worms,and trojans-2.5 days
    7. Malware-2 days
    8. Botnets- 2 days

There are many new endpoints in today's complex networks; they include hand-held devices.

1. **Endpoint protection**: It is an often-ignored area but it is IP-based printers, although they are passive devices, are also one of the endpoints.
2. **Secure coding:** These practices are important because they are a good mitigation control to protect organizations from "Malicious Code" inside business applications.
3. **HR checks:** These are important prior to employment as well as after employment.
4. **Access controls:** These are always important, for example, shared IDs and shared laptops are dangerous. (for confidential and sensitive data).
5. **Importance of security governance:** It cannot be ignored - policies, procedures and their effective implementation cannot be over-emphasized.

Organizational Implications of Software Piracy

- Use of pirated software is a major risk area for organizations.
  From a legal standpoint, software piracy is an IPR violation crime.
- Use of pirated software increases serious threats and risks of cybercrime and computer security when it comes to legal liability.

The most often quoted reasons byemployees, for use of pirated software, are as follows:

1. Pirated software is cheaper and more readilyavailable.
2. Manyothers use pirated software anyways.
3. Latest versions are available faster when pirated software is used.

Web Threats for Organizations: The Evils and Perils

- Internet and the Web is the way of working today in the interconnected digital economy. More and more business applications are web based, especially with the growing adoption of cloud computing.
- There is inevitable dependence on the Internet. (purchase, audio, video, weather forecast, etc.,).
- Therefore, cybercriminals find it convenient to use the Internet for committing crimes.

Web threats for organizations:

1. Overview of Web Threats to Organizations:

- The Internet has engulfed us! Large number of companies as well as individuals have a connection to the Internet. Employees expect to have Internet access at work just like theydo at home.
- IT managers must also find a balance between allowing reasonable personal Internet use at work and maintaining office work productivity and work concentration in the office.

2. Employee Time Wasted on Internet Surfing:

- This is a very sensitive topic indeed, especially in organizations that claim to have a "liberal culture." Some managers believe that it is crucial in today's business world to have the finger on the pulse of your employees.
- People seem to spend approximately 45-60 minutes each working day on personal web surfing at work.
- Organization need to discipline an employee for Internet misuse,
  1. Safe Computing Guidelines/Internet Usage Guidelines.
  2. Organization need software installed, which monitor employee's Internet activities in the background. Cookies store the surfing activities.

3. Enforcing Policy Usage in the Organization:

- An organization has various types of policies. A security policy is a statement produced by the senior management of an organization, or by a selected policy board or committee to dictate what type of role securityplays within the organization.

4. Monitoring and Controlling Employee's Internet Surfing:

- A powerful deterrent can be created through effective monitoring and reporting of employees' Internet surfing.
- Even organizations with restrictive policies can justify a degree of relaxation.
- for example, allowing employees to access personal sites only during the lunch hour or during specified hours.
- Managers get insight into employee's web use, in close association of "cookies" with website visited during Internet Surfing.
- HR investigations becomes possible- managers giving a broad picture of company-wide usage patterns and productivity.

5. Keeping Security Patches and Virus Signatures Up to Date:

- Updating security patches and virus signatures have now become a reality of life, a necessaryactivity for safety in the cyberworld!
- Keeping security systems up to date with security signatures, software patches, etc. is almost a nightmare for management.
- Doing it properly and regularly absorbs a significant amount of time, but at same time, not doing it properly exposes IT systems to unnecessaryrisk.

6. Surviving in the Era of Legal Risks:

- Most organizations get worried about employees visiting inappropriate or offensive websites.
- Downloading Children Pornography, Pirated Software, inappropriate images, irresponsible comments made by employee on public Internet forum can be a breach for liabilityand confidentiality guidelines.
- Serious legal liabilities arise for businesses from employee's misuse/ inappropriate use of the Internet.
- It is quite challenging to address and reduce risks, however organizations with effective web filtering and monitoring can provide reassurance and reduce risks.

7. **Bandwidth Wastage Issues:**
    - Today's applications are bandwidth hungry; there is an increasing image content in messages and that too, involving transmission of high-resolution images.
    - There are tools to protect organization's bandwidth by stopping unwanted traffic before it even reaches your Internet connection.

8. **Mobile Workers Pose Security Challenges:**
    - Most mobile communication devices for example, the PDAs and RIM BlackBerries has raised security concerns with their use.
    - Mobile workers use those devices to connect with their company networks when they move. So the organizations cannot protect the remote user system as a result workforce remains unprotected.
    - We need tools to extend web protection and filtering to remote users, including policy enforcement.

9. **Challenges in Controlling Access to Web Applications:**
    - Today, a large number oforganizations' applications are web based.
    - There will be more in the future as the Internet offers a wide range of online applications, from webmail or through social networking to sophisticated business applications.
    - Employees often tend to use these applications to bypass corporate guidelines on security.
    - For example, to access personal E-mail or upload company data to services outside company control; sometimes, employees may use their personal mail id to send business sensitive information (BSI) for valid or other reasons. It leads to data security breach.
    - The organizations need to decide what type of access to provide to employees.

10. **The Bane of Malware:**
    - Manywebsites contain malware. Such websites are a growing securitythreat.
    - Although most organizations are doing a good job of blocking sites that declared as dangerous; cyber attackers, too, are learning.
    - Criminals change their techniques rapidlyto avoid detection.
    - The consequences of infection are severe compared with any kind of malware.

11. **The Need for Protecting Multiple Offices and Locations:**
    - Delivery from multi-locations and teams collaborating from multi-locations to deliver a single project are a common working scenario today.
    - Most large organizations have several offices at multiple locations.
    - Protecting information security and data privacy at multiple sites is indeed a major issue because protecting single site itself is a challenge.
    - In such scenario Internet-based hosted service can easilyprotect many offices.

Security and privacy implications from cloud computing

- Cloud computing is one of the top 10 Cyber Threats to organizations. There are data privacy risks through cloud computing. Organizations should think about privacy scenarios in terms of "user spheres".
- There are three kinds of spheres and their characteristics:
    1. User sphere: Here data is stored on user's desktops, PCs, laptops, mobile phones, Radio Frequency Identification (RFID) chips, etc. Organization's responsibility is to provide access to users and monitor that access to ensure misuse does not happen.
    2. Recipient sphere: Here, data lies with recipients: servers and databases of network providers, service providers or other parties with whom data recipient shares data.

Organizations responsibility is to minimize users privacy risk by ensuring unwanted exposure of personal data of users does not happen.

3. Joint sphere: Here data lies with web service provider's servers and databases. This is the in-between sphere where it is not clear to whom does the data belong. Organization responsibility is to provide users some control over access to themselves and to minimize users futures privacy risk.

Social Media Marketing: Security Risks and Perils for Organizations

- Social media marketing has become dominant in the industry. According to fall 2009 survey by marketing professionals; usage of social media sites by large business-to-business (B2B) organizations shows the following:
  - Facebook is used by 37% of the organizations.
  - LinkedIn is used by 36% of the organizations.
  - Twitter is used by 36% of the organizations.
  - YouTube is used by 22% of the organizations.
  - MySpace is used by 6% of the organizations
- Although the use of social media marketing site is rampant, there is a problem related to "social computing" or "social media marketing" – the problem of privacy threats.
- Exposures to sensitive PI and confidential business information are possible if due care is not taken by organizations while using the mode of "social media marketing."

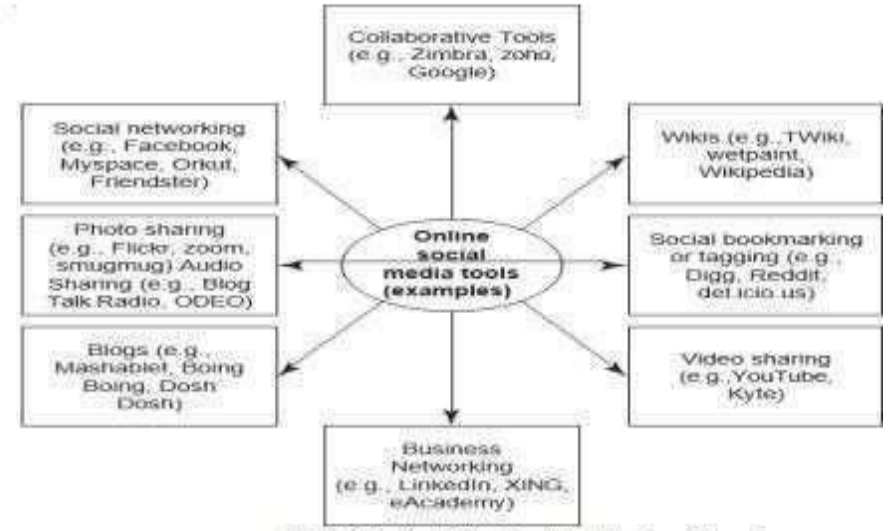


FIG: Social Media Marketing Tools

Understanding Social Media Marketing:

- Most professionals today use social technologies for business purposes.
- Most common usage include: marketing, internal collaboration and learning, customer service and support, sales, human resources, strategic planning, product development.

Following are the most typical reasons why organizations use social media marketing to promote their products and services:

1. To be able to reach to a larger target audience in a more spontaneous and instantaneous manner without paying large advertising fees.

2. To increase traffic to their website coming from other social media websites by using Blogs and social and business-networking. Companies believe that this, in turn, may increase their "page rank" resulting in increased traffic from leading search engines.
3. To reap other potential revenue benefits and to minimize advertising costs because social media complements other marketing strategies such as a paid advertising campaign.
4. To build credibility by participating in relevant product promotion forums and responding to potential customers' questions immediately.
5. To collect potential customer profiles. Social media sites have information such as user profile data, which can be used to target a specific set of users for advertising.

There are other tools too that organizations use; industrypractices indicate the following:

1. Twitter is used with higher priority to reach out to maximum marketers in the technology space and monitor the space.
2. Professional networking tool LinkedIn is used to connect with and create a community of top executives from the Fortune 500.
3. Facebook as the social group or social community tool is used to drive more traffic to Websense website and increase awareness about Websense.
4. YouTube (the video capability tool to run demonstrations of products/services, etc.) is used to increase the brand awareness and create a presence for corporate videos.
5. Wikipedia is also used for brand building and driving traffic.

- There are conflict views about social media marketing some people in IT say the expensive and careless use of it. Some illustrate the advantages of it with proper control of Securityrisk

Best Practices with Use of Social Media Marketing Tools:

1. **Establish a Social Media Policy:**
    - Use of personal blogging for work related matters should be monitored and minimized (Internet Surfing).
    - Use of policies and implementation of policy-based procedures are always essential.
    - Once the policy is created, employers should communicate it to employees and should enforce its implementation through continuous monitoring
2. **Establish Firm Processes based on the Policy:**
    - Network Security administrators need to remain up to date about the most recent risks on the Web.
    - There is a strong need to establish firm processes that are systematically linked to daily workflows.
        - For Example: Administrators should ensure that the latest security updates are downloaded and identify network attacks in time or to avoid them altogether.
3. **Establish the Need-Based Access Policy:**
    - It becomes possible to control and monitor access to critical data and to track such access at anytime.
    - This reduces the risk of information falling into wrong hands through unauthorized channels.
    - Policies should not be treated as one-time activity.
    - The policies must be kept updated and adapt themto changing circumstances.
4. **Blocking the Infected files:**
    - URL filters allow organizations to block access to known Malware and Phishing Websites.

- Access blocking can also be applied to anyother suspicious site on the Internet.
- The filter function should be kept continuously up to date by maintaining so-called black-and-White-listed Websites.

5. Use of Firewalls:

- Firewalls helps organizations keep their securitytechnologyup to date.
- Some firewalls provides a comprehensive analysis of all data traffic.
- Deep inspection of Network traffic makes it possible to monitor the type of data traffic, the websites from which it is coming, to know the web browsing patterns and peer-to-peer applications to encrypted data traffic in SSL tunnel.
- The firewall decrypt the SSL data stream for inspection and encrypt it again before forwarding the data to the Network.
- This results in effective protection of Workstations and other endpoints, internal networks, hosts and servers against attacks within the SSL tunnels.

6. Protection against vulnerability:

- It is possible bycarefully planning vulnerability scanning and penetration testing.
- Vulnerabilities present a huge challenge to anycorporate network.
- An Intrusion Prevention System (IPS) serves as a protective barrier to the corporate network.
- An IPS automatically prevents attacks byworms, viruses and other malware.
- Once an attack is identified, the IPS immediately stops it and prevents it from spreading in the network.

7. Define Access to Business Application:

- Define "need-based" access to business applications that reside on corporate networks as well on the external sites.
- There is a phenomenal rise in workforce mobility-this makes it even more important to assign rights for defining all network access centrally.
- On the user level, a strong authentication via single sign-on makes the administrator's work easier.
- As a result, a single login makes it possible for users to access only the network areas and services for which they are authorized.

8. Securing the Intranet:

- The Intranets are not spared byCyberattacks.
- Therefore, securing the Intranets should also be included in the protection activities.
- The Intranet of every company contains highly sensitive information pertaining to the business areas.
- These areas need to be isolated from the rest of the internal network by using the firewalls to segment the Intranet.
- This enables segregation of departmental Intranets.
- For example, a company can segregate departments such as finance and accounting from the rest of the Intranet and thereby prevent infections from penetrating these critical segments of the corporate network.
- Firewall with two demilitarized zone (DMZ) networks.

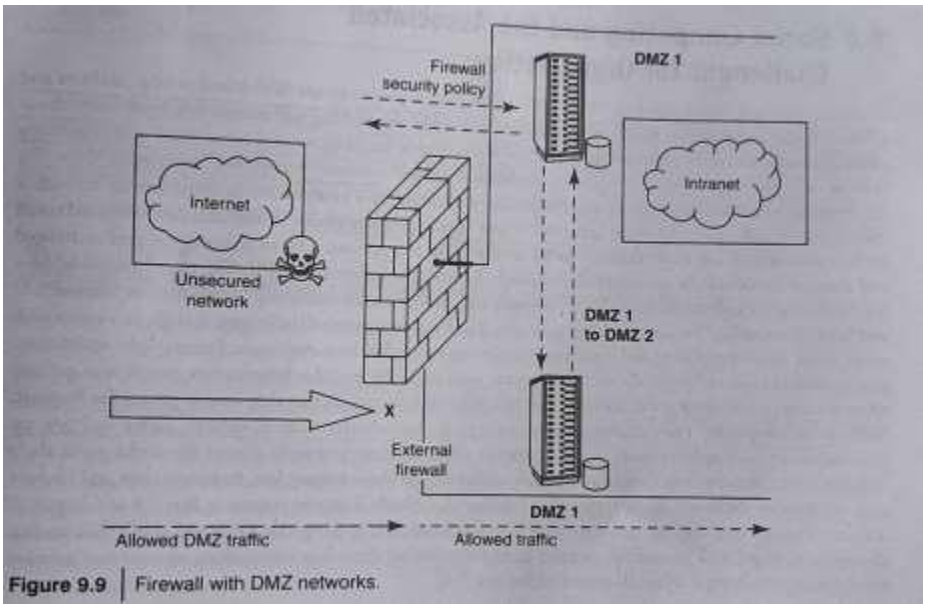


Figure 9.9 | Firewall with DMZ networks.

9. Include mobile devices in the security policy:

- It is common for users to navigate social web services with mobile devices such as laptops, PDA and Smartphones.
- The same devices are used bythe users to log into the corporate network.
- The corporate security department therefore, needs to include mobile devices in the securitypolicies.
- For example, with the assessment function by checking the login device for the required securitysettings and for the presence of securityrelevant software packages.
- Through this function, it can be checked whether the proper and latest host firewall is installed and whether both the OS and Antivirus software as well as all patches are up to date.

10. Use of centralized Management:

- Administrators can manage, monitor and configure the entire network and all devices using a single management console.
- Theycan also monitor user activities on the network by viewing reports.
- For example, System administrators will be able to know who has accessed, which data, at what time.
- This allows preventing attacks more efficiently and provide more protection for corporate applications from risk.
- The Organizational best practices are:
    - Organization-wide information systems securitypolicy;
    - Configuration/change control and management;
    - Risk assessment and management;
    - Standardized software configurations that satisfy the information systems security policy;
    - Securityawareness and training;
    - Contingency planning, continuityof operations and disaster recoveryplanning;
    - Certification and accreditation.

Social Computing and the Associated Challenges for Organizations

- Social Computing is also known as "Web 2.0".
- It empowers people to use Web-based products and services.
- It helps thousands of people across the globe to support their work, health, getting entertained and citizenship tasks in a number of innovative ways.
- In the modern era-we are "constantly Connected" to business is "24 X 7", the business where World never sleeps, people and organizations are appreciating the "Power of Social Media.
- In this process, a lot of Information gets exchanged and some of that could be confidential, Personally Identifiable Information (PII), etc.
- This would be a gold mine for the Cybercriminals.
- Getting too used to readily available information, people may get into the mode of not questioning the accuracy and reliability of information that theyreadily get from the Internet.
- Social Computing, new threats are emerging; those relate to security, safetyand privacy.
- Social Computing is related to Social Media Marketing because business leaders in product development, marketing and sales view social computing as an integral part of the evolving enterprise channel strategy.

Cybercrime and Cyber terrorism: Introduction:

Cyberattacks can come in the form of viruses, malware, email phishing, social media fraud - the spectrum of cyber threats is limitless. We are more interconnected than ever before, but for all of the advantages, that connectivity leaves us vulnerable to the risks of fraud, theft, abuse, and attack. Cybercrime can have wide-ranging impacts, at the individual, local, state, and national levels.

Organized cybercrime, state-sponsored hackers, and cyber espionage can pose national securityrisks to our countryand our critical infrastructure.

Transportation, power, and other services may be disrupted by large scale cyber incidents. The extent of the disruption is highly uncertain as it will be determined by many unknown factors such as the target and size of the incident.

Vulnerability to data breach and loss increases if an organization's network is compromised. Information about a company, its employees, and its customers can be at risk.

Individually-owned devices such as computers, tablets, mobile phones, and gaming systems that connect to the Internet are vulnerable to intrusion. Personal information may be at risk without proper security.

What is cyber crime and cyber terrorism?
cyber terrorism is defined by follow: "previously planned, politically motivated attack. against information, computer systems, computer programs and data that result with. violence against targets that are not military (civilian) by the sub - national groups or secret.

What is the impact of cyber terrorism?
An effect, most commonly violence, service disruptions, physical damages, psychosocial impacts, economic damages, or data breaches. A target, most commonly civilians, information and

communication technology (ICT), data sources, government agencies, nongovernment organizations, or physical infrastructure.

Cybercrime and Cyber Terrorism

As we become more connected and reliant on technology, we become morevulnerable to cyberattacks.

Cyberattacks can come in the form of viruses, malware, email phishing, social media fraud - the spectrum of cyber threats is limitless. We are more interconnected than ever before, but for all of the advantages, that connectivity leaves us vulnerable to the risks of fraud, theft, abuse, and attack. Cybercrime can have wide-ranging impacts, at the individual, local, state, and national levels.

- Organized cybercrime, state-sponsored hackers, and cyber espionage can pose national security risks to our country and our critical infrastructure.
- Transportation, power, and other services may be disrupted by large scale cyber incidents. The extent of the disruption is highly uncertain as it will be determined by many unknown factors such as the target and size of the incident.
- Vulnerability to data breach and loss increases if an organization's network is compromised. Information about a company, its employees, and its customers can be at risk.
- Individually-owned devices such as computers, tablets, mobile phones, and gaming systems that connect to the Internet are vulnerable to intrusion. Personal information may be at risk without proper security.

Take Action Before Cybercrime and Cyber Terrorism

We can increase your chances of avoiding cyber risks by setting up the proper controls and sharing information with your friends and family when known risks exist.

Lock or log-off your computer when you are away from it. This prevents another person from waiting for you to leave and then sitting down at your computer and accessing all of your information.

Look for signals that you are using a secure webpage. A secure site encrypts or scrambles personal information so it cannot be easily intercepted. Signals include a screen notice that says you are on a secure site, a closed lock or unbroken key in the bottom corner of your screen, or the first letters of the Internet address you are viewing changes from "http" to "https."

Look for a privacy policy statement or seal that indicates the site abides by privacy standards. Take time to read how your privacy is protected.

Take Action on Your Computer and Handheld Devices

- Stay protected while connected. Only connect to the Internet over secure, password-protected networks. Avoid free internet with no encryption. If you do use an unsecure public access point, avoid sensitive activities that require passwords or credit cards.
- If you are unsure of who an email is from, do not respond and do not click on any links or attachments.
- Do not respond to online requests for Personally Identifiable Information (PII); most organizations – banks, universities, companies, etc. – do not ask for your personal information over the Internet. PII includes, but is not limited to, your full name, social security number, address, date of birth, place of birth, driver's license number, vehicle registration plate number, credit card numbers, and physical appearance.
- Limit who you are sharing information with by reviewing the privacy settings on your social media accounts. Disable geotagging, which allows anyone to see where you are – and where you are not.

- Password-protect all devices that connect to the Internet and user accounts. Create a strong password that contains multiple characters, numbers, capitalized letters, and symbols.
- Do not use the same password twice. Choose a password that means something to you and you only and change your passwords on a regular basis.
- Enable multi-factor authentication to ensure that the only person with access to your accounts is you.
- Apps can be a source for identity theft and malicious activity. Only download apps from trusted sources. Check your app permissions and only allow what is necessary. Delete apps that you no longer use or need.
- If you see something suspicious, report it to the proper authorities.

Be Safe During Cybercrime or Cyber Terrorism

If you know that you are the victim of a cyber-attack, or if you know that an attack has occurred, you should take actions to ensure that your personal data is protected. Check to make sure the software on all of your systems is up-to-date. Run a scan to make sure your system is not infected or acting suspiciously. If you find aproblem, disconnect your device from the Internet and perform a full system restore.

Be Safe At Home

- Disconnect your device (computer, gaming system, tablet, etc.) from the Internet. By removing the Internet connection, you prevent an attacker or virus from being able to access your computer and perform tasks such as locating personal data, manipulating or deleting files, or using your device to attack others.
- If you have anti-virus software installed on your computer, update the virus definitions (if possible), and perform a manual scan of your entire system. Install all of the appropriate patches to fix known vulnerabilities.

Be Safe At Work

- If you have access to an information technology department, contact them immediately. The sooner they can investigate and clean your computer, the less damage to your computer and other computers on the network.
- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.

Be Safe if Your PII is Compromised

- Immediately change all passwords, beginning with your financial passwords. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.
- If you believe the compromise was caused by malicious code, disconnect your computer from the Internet.
- Restart your computer in safe mode and perform a full system restore.
- Contact companies, including banks, where you have accounts as well as credit reporting companies.
- Close any accounts that may have been compromised. Watch for any unexplainable or unauthorized charges to your accounts.

Take Action After Cybercrime or Cyber Terrorism

After a cyber-attack that personally impacts your information or your organization's information, you should take actions to ensure that your data is protected and that appropriate reports are made to local law enforcement. You can also report online crime or fraud to your local Cyber crime department or the Internet Crime Complaint Center. Report identity theft to the Federal Trade Commission. Report phishing scams to the National Cybersecurity Communications and Integration Center.

If your Personally Identifiable Information (for example your social security number) was compromised, consider other information that may be at risk. Depending on what information was stolen, you may need to contact other agencies; for example, if someone has gained access to your Social Security number, contact the Social Security Administration. You should also contact the Division of Motor Vehicles if your driver's license or car registration has been stolen.

Intellectual property in the cyberspace:

In common use, property is simply 'one's own thing' and refers to the relationship between individuals and the objects which they see as being their own to dispensewith as they see fit. Scholars in the social sciences frequently conceive of property asa 'bundle of rights and obligations'. They stress that property is not a relationship between people and things, but a

relationship between people with regard to things. Property is often conceptualized as the rights of 'ownership' as defined in law. Private property is that which belongs to an individual; public property is that which belongs to a community collectively or a State. Property is usually thought of in terms of a bundle of rights as defined and protected by the sovereign.

Traditionally, that bundle of rights includes: z control use of the property z benefit from the property (e. g.: mining rights and rent) z transfer or selling of the property z exclude others from the property Intellectual Property Protection in Cyberspace .

The term intellectual property reflects the idea that this subject matter is the product of the mind or the intellect, and that intellectual property rights may be protected at law in the same way as any other form of property. Intellectual property laws are territorial such that the registration or enforcement of IP rights must be pursued separately in each jurisdiction of interest.

However, these laws are becoming increasingly harmonised through the effects of international treaties such as the Berne Convention, Paris Convention and WTO Agreement on TradeRelated Aspects of Intellectual Property Rights. Intellectual property laws confer a bundle of exclusive rights in relation to the particular form or manner in which ideas or information are expressed or manifested, and not in relation to the ideas or conceptsthemselves.

The term "intellectual property" denotes the specific legal rights which authors, inventors and other IP holders may hold and exercise, and not the intellectual work itself. Intellectual property laws are designed to protect different forms of intangible subject matter, although in some cases there is a degree of overlap. Like other forms of property, intellectual property (or rather the exclusive rights which subsist in the IP) can be transferred or licensed to third parties. There are various kinds of tools of protection that come under the umbrella term 'intellectual property'. Important among these are the following: z Patents z Trademarks z Geographical Indications z Layout Designs of Integrated Circuits z Trade Secrets z Copyrights z Industrial Designs Out of this tool kitty mainly it is copyright and trademark which are of relevance when we discuss intellectual property protection in cyberspace. Before proceeding to discuss the exact application of IP laws and their implication in cyberspace, it becomes imperative to know in some greater detail about them.

After reading this unit, you should be able to: z explain the term intellectual property; z describe the basic concept of copyright and the rights included in the term copyright; z explain infringement of copyright and what are the remedies; z explain the concept of trademark the rights of trademark and

remedies for their search; and z describe the challenges faced by IPR in cyberspace.
Intellectual Property in Cyberspace. Basic Concept Copyright is a right given by law to the creators of literary, dramatic, musical and artistic works and producers of cinematograph films and sound recordings to do or authorize the doing of certain acts with regard to their creations. It is a kind of protection against unauthorized use or misuse of a work, but for a
limited duration.

Generally the rights include the rights of authorship, reproduction, distribution, communication to the public, broadcasting, adaptation and translation. The exact nomenclature and scope of the rights may vary from country to country and from a class of work to another class of work. However, international treaties such as the Berne Convention for the protection of Literary and Artistic Works and the Agreement on Trade Related Aspects of Intellectual Property Rights have brought in some kind of harmonization in these rights. In India, copyright is governed by the Copyright Act, 1957, the Copyright Rules, 1958 and the International Copyright Order, 1999. The Copyright Act provides the basic law so far as copyrights are concerned, the Copyright Rules contain the rules and regulations as well as various procedures and the International Copyright Order extends copyright protection to works of nationals of specified foreign countries.

The Copyright Act classifies the works in which copyright subsists in India in to the following three classes:

(a) literary, dramatic, musical and artistic works

(b) cinematograph films, and

(c) sound recordings.

The scope of 'literary work' includes any "work which is expressed in print or writing, irrespective of the question whether the quality or style is high". It also includes computer programs and computer databases. Dramatic work includes any piece for recitation, choreographic work or entertainment in dumb show, the scenic arrangement or acting, form of which is fixed in writing or otherwise but does not include a cinematograph film. Musical work means a work consisting of music and includes any graphical notation of such work but does not include any words or any action intended to be sung, spoken or performed with the music. Artistic work means a painting, a sculpture, a drawing (including a diagram, map, chart or plan), an engraving or a photograph, whether or not any such workpossesses artistic quality; a work of architecture; and any other work of artistic craftsmanship.

The Copyright Act defines cinematograph film as "any work of visual recording on any medium produced through a process from which a moving image may be produced by any means and, includes a sound recording accompanying such visual recording". Sound recording (phonogram) is a recording of sounds from which sounds can be produced regardless of the medium on which such recording is made or the method by which the sounds are produced. Please answer the following Self Assessment Question. Self Assessment Question 1 Spend 2 Min. Copyright is governed by Act.
Intellectual Property Protection in Cyberspace 8 8.3.2 Rights Included in the term 'Copyright' Copyright is a bundle of rights and this bundle can be broadly classified into two categories, viz. economic rights and moral rights. Economic rights are so called because "they imply as a rule that within the limitations set by the copyright law the owner of the copyright may make all public use of the work conditional on payment of remuneration".

These rights enable the copyright owner to reap economic returns for his work. The major economic rights available in the Indian copyright Act are the following:

(a) Right of Reproduction
(b) Right to Issue Copies of a Work
(c) Rights of Public Performance
(d) Right of Communication to the Public
(e) Adaptation Right
(f) Translation Right Right of reproduction is the most fundamental of all economic rights. The right envisages that copyright owner has the exclusive right to authorize the making of one or more copies of a work or of a substantial part of it in any material form, including sound and visual recording. The most common kind of reproduction is printing an edition of a book. Storing of a work in any medium by electronic means is also reproduction. The Copyright Act gives the right of reproduction in all classes of works. Moral Rights are generally provided with a view to assert the authorship on a work and also to uphold the right of integrity. The Indian Copyright Act provides this as special rights of authors to claim authorship of the work and to restrain or claim damages in respect of any distortion, mutilation, modification or other act in relation to the said work which is done before the expiration of the term of copyright if such distortion, mutilation, modification or otheract would be prejudicial to his honour or reputation. Moral rights are independent of the economic rights and remain with the author even after he has transferred his economic rights. In the era of digital technologies, moral rights, particularly right of integrity, are very necessary to safeguard against misuse and distortion of an author's work.

Copyright, being a property right, can be transferred or assigned to another person. It can also be inherited during the time it exists. Without transferring or assigning, a copyright owner can license specified uses by others. 8.3.3 Infringement of Copyright and Remedies Thereof Any copying or duplication, adaptation, translation, public performance, communication to the public or broadcast done without the authorization of the copyright owner, or even where any work has been licensed or assigned, any violation of the conditions of the licence or assignment constitutes copyright infringement. Any import of infringing copies also constitutes copyright infringement. Even such copies made outside India cannot be imported into India without infringing copyright where such copies, if made in India, would infringe copyright, even if it may not be an infringement in the country of origin.

Since copyright is a proprietary right, the owner has to administer his own rights. The Copyright Act provides for collective Intellectual Property in Cyberspace 9 administration of rights through registered copyright societies. These societies have to be formed voluntarily by the copyright owners. Only the owner of copyright or the society who have the rights can institute civil and criminal proceedings against infringement of his works. Civil remedies include injunction, and damages.

Copyright infringement is also a cognizable offence. Copyright infringement is punishable with imprisonment for a term ranging from six months to three years and with a fine ranging from Rs. 50,000 to Rs. Two lakh. District Courts have been given jurisdiction to try the suits relating to copyright violation within the vicinity of which the owner of the
copyright resides or carries on business. 8.3.4 Limitations/Exceptions to Copyright The rights granted by copyright are exclusive in nature. This exclusivity is sometimes criticised as monopoly in favour of the right owners.

Therefore, in order to balance these opposing private and public interests the legislature provides the remedy in the form of drawing limitations/exceptions to copyright. This is achieved by two means; firstly, limiting the duration in which a work enjoys copyright protection, and secondly, allowing

certain uses without specific authorization by the owner of copyrights, known as fair use provisions in copyright parlance. Copyright is an intellectual property right and like all other intellectual property rights it is for a limited duration.

This limitation emanates from the basic concept of intellectual property right that while creators of intellectual property have the right to control the reproduction and other uses of their works, they being essential elements in the scientific and cultural progress of humanity, the society has the right to access and share the same so that social and cultural life of humanity gets enriched.

While the Berne Convention provides for a minimum period of protection which is life term of the author plus 50 years thereafter, national governments are free to provide a longer term of protection. In India, original literary, dramatic, musical and artistic works enjoy copyright protection for the lifetime of the author plus 60 years if they are published within the lifetime of the author.

Many types of exploitation of a copyrighted work which are for social purposes such as education, religious ceremonies, and so on are exempted from the operation of the rights granted in the Act. For example, playing music at religious ceremonies, including marriage processions and marriage festivities, official functions of central and state governments and local bodies will not be affected by copyright.

This is done in keeping with the social and cultural traditions of the country. 8.3.5 Registration of Copyright The Copyright Act provides for registration of works. However, the registration under the Act is voluntary and not obligatory. Registration does not itself confer copyright but the particulars entered in the Register of Copyright maintained inthe Copyright Office constitute prima facie evidence of ownership of copyright in copyright cases. As per the provisions of the Act, copyright subsists in any work as soon as it is created, without any formality like registration being observed. 8.3.6 International Nature ofCopyright Protection Copyrights are national in nature.

This means that your rights are recognised by your national laws and extend to the territorial limits of your country. However, international treaties like the Berne Convention for the Protection of Literary and Artistic Works Intellectual Property Protection in Cyberspace 10 (1886) the Universal Copyright Convention (1952) and the Agreement on Trade Related Aspects of Intellectual Property Rights (1994) ensure protection of copyrights of nationals of a member country in all other member countries. Through the principle of 'National Treatment' it is ensured that foreigners if they are nationals of a membercountry, are given the same rights enjoyed by the nationals, except in the matter of term of protection.

India is part of the international copyright regime through its membership of Berne Convention for the Protection of Literary and Artistic Works, Convention Establishing the

World Intellectual Property Organization (WIPO), Universal Copyright Convention, Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of Their Phonograms, Multilateral Convention for the Avoidance of Double Taxation of Copyright Royalties and Additional Protocol, and the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS)

The ethical dimension of cybercrimes the psychology:

We saw that the 'good life' is what ethical action seeks to protect and promote. We'll say more later about the 'good life' and why we are ethically obligated to care about the lives of others beyond ourselves. But for now, we can define an ethical issue as 'important' or 'significant' when its associated harms or benefits have a substantial possibility of making a difference to certain individuals' chances of having a good life, or the chances of a group to live well: that is, to

flourish in society together. Some harms and benefits are not ethically significant.

Say I prefer Coke to Pepsi. If I ask for a Coke and you hand me a Pepsi, even if I am disappointed, you haven't impacted my life in any ethically significant way. Some harms and benefits are too trivial to make a meaningful difference to how our life goes. Also, ethics implies human choice; a harm that is done to me by a wild tiger or a bolt of lightning might be very significant, but won't be ethically significant, for it's unreasonable to expect a tiger or a bolt of lightning to take my life or welfare into account.3 In many technical contexts, such as the engineering, manufacture, and use of aeronautics, nuclear power containment structures, surgical devices, buildings, and bridges, it is very easy to see the ethically significant harms that can come from poor technical choices, and very easy to see the ethically significant benefits of choosing to follow the best technical practices known to us.

All of these contexts present obvious issues of 'life or death' in practice; innocent people will die if we disregard public welfare and act negligently or irresponsibly, and people will generally enjoy better lives if we do things right. Because 'doing things right' in these contexts preserves or even enhances the opportunities that other people have to enjoy a good life, good technical practice in such contexts is also ethical practice. A civil engineer who willfully or recklessly ignores a bridge design specification, resulting in the later collapse of said bridge and the deaths of a dozen people, is not just bad at his or her job. Such an engineer is also guilty of an ethical failure—and this would be true even if they just so happened to be shielded from legal, professional, or community punishment for the collapse.

In the context of cybersecurity practice, the potential harms and benefits are no less real or ethically significant, up to and including matters of life and death. But due to the fact that cybersecurity efforts are often carried out 'behind the scenes,' largely hidden away from customers, clients, and other users, the ethical nature of cybersecurity practice can be harder to recognize. This part of the module seeks to make these issues more visible.

Mindset and skills of hackers and other cybercriminals:

Alok (name changed on request) is in his early teens, not the age when he should be making thousands of dollars. Alok is a hacker who lives on the dangerous by-lanes of the internet— the dark web. Accessible only through browsers designed to promote anonymity and confuse law enforcement, the dark web is where the nefarious elements of the internet hang out. The baby-faced Alok has been working with a hacker collective on the dark web for nearly three years now. In those three years, he has been party to several instances of theft and trading, particularly of credit card information, on the dark web and its marketplaces. He was never a leader, but one of the foot soldiers, yet he managed to earn bitcoins that are now worth thousands of dollars. Alok hides his wealth from his parents.

These days, Alok is in the throes of a moral crisis. It may have paid him well, but he is not sure if he wants to continue being what those in the security business calls a black hat hacker—someone who uses his skills for negative, often illegal ends. As he grows up, Alok is going through the realisation of his own power and of the ways in which he can use it.

Meet the hackerIf the mental picture that lights up in your mind when you hear of Alok the hacker is of a young, bespectacled guy sitting in a dark room, with his face lit up by the bluish glow of his computer monitor, you are not too far away from reality. That's where the journey of most hackers start—staying up in the middle of the night, trying different things, finding and learning new ways

to manipulate code and find vulnerabilities.

Like Alok, somewhere along the way, they see a fork on the road, one that could take them towards using their power to make code dance to their tunes for the good, the other that takes them to the direction where they could wreak havoc. It's 2017 and coding is power and exceptional coders have an inordinate amount of power. Efforts to target cyber installations of ISIS is just one such example.

For most people, the hacker is a mysterious being. There is so little that the person on the street knows about these digital lock-pickers and much of the little they do know has been influenced by how the hacker is portrayed in popular culture.

The term hacker itself has become more complicated over the years. Its usage— alternating between black hat and white hat (the good guys)—means that the meaning oscillates between something of an outlaw in the Wild West of the internet while at the same time conjuring up images of the sheriff of the town as well.

The Hacker mind Why do hackers, well, hack? It often starts with a need for thrills, for validation. It is not always the money on offer that attracts them to turn rogue; it is a need for the adrenalin rush that comes from breaking impenetrable defences and proving themselves to other hackers. According to several coders I have met, that moment of triumph of knowing of their own power, is something of a crucial rite of passage.

Alok, the young hacker, remembers his first hack, finding a vulnerability in how a startup in Bangalore stored user data and getting a T-shirt as swag from the company after he reached out to them and warned them about it. The sense of idealism and an overwhelming

belief in the power of technology to set right the ills of the society is real and drives many young coders. Hackers tend to havean acute, heightened sense of what is right and what is wrong, and much of their behaviour is based ..

That is what, in particular, leads to the formation of hacktivist collectives like Anonymous which tries to correct what theyclaim are social or injustices

Hackers will exert huge influence over our lives as we move towards an even more connected world. Civil society and governments need to invest in understanding them and trying to channelise their power in making the world a better place.

UNIT-V
Privacy Issues

Basic Data Privacy Concepts

Fundamental Concepts:

Data Privacy:

Data Privacy or Information privacy is a part of the data protection area that deals with the proper handling of data focusing on compliance with data protection regulations.

Data Privacy is centered around how data should be collected, stored, managed, and shared with any third parties.

Elements of Data Privacy

- Data Privacyor Information privacy encompasses 3 elements:
- Right of an individual to be left alone and have control over their personal data
- Procedures for proper handling, processing, collecting, and sharing of personal data
- Compliance with data protection laws.

Data Privacy Vs Data Security

Data Privacy

- **Data Privacy** focuses on the **rights of individuals**, the purpose of data collection and processing, privacy preferences, and the way organizations govern personal data of data subjects.
- It focuses on how to collect, process, share, archive, and delete the data in accordance with the law.

Data Security

- **Data Security** includes a set of standards and different safeguards and measures that an organization is taking in order to prevent any third party from unauthorized access to digital data, or any intentional or unintentional alteration, deletion or disclosure of data.
- It focuses on the protection of data from malicious attacks and prevents the exploitation of stolen data (data breach or cyber-attack). It includes Access control, Encryption, Network security, etc.

Data Privacy Attacks / Data Breaches

Data Breach:

A data breach is a security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.

Types of Data Breaches:

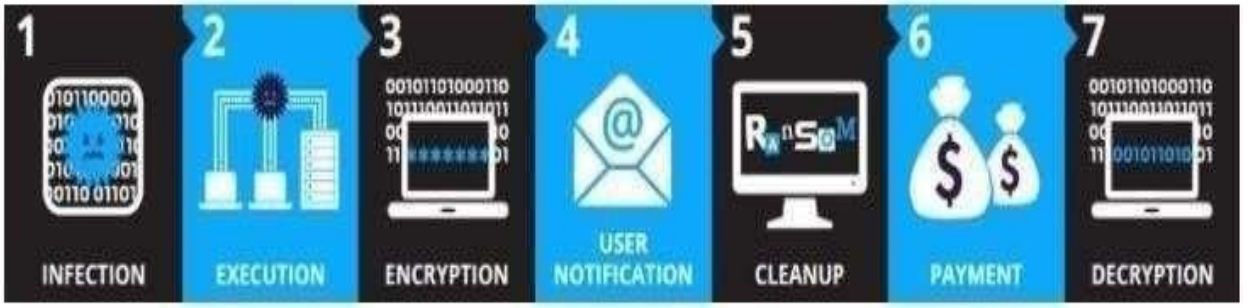
1. Stolen Information
2. Ransomware
3. Password Guessing
4. Recording Key Strokes
5. Phishing
6. Malware or Virus
7. Distributed Denial of Service (DDoS)

Stolen Information:

Stolen data may involve sensitive, proprietary, or confidential information such as credit card numbers, customer data, trade secrets, or matters of national security.

Ransomware:

Ransomware is a type of malware attack in which the attacker locks and encrypts the victim's data, important files and then demands a payment to unlock and decrypt the data.



Ransomware seven-stage attack

1. **Infection**—Ransomware is covertlydownloaded and installed on the device.
2. **Execution**—Ransomware scans and maps locations for targeted file types, including locally stored files, and mapped and unmapped network-accessible systems. Some ransomware attacks also delete or encrypt any backup files and folders.
3. **Encryption**—Ransomware performs a key exchange with the Command-and-Control Server, using the encryption key to scramble all files discovered during the Execution step. It also locks access to the data.
4. **User Notification**—Ransomware adds instruction files detailing the pay-for-decryption process, then uses those files to display a ransom note to the user.
5. **Cleanup**—Ransomware usually terminates and deletes itself, leaving only the payment instruction files.
6. **Payment**—Victim clicks a link in the payment instructions, which takes the victim to a web page with additional information on how to make the required ransom payment.
7. **Decryption**—After the victim pays the ransom, usually via the attacker's Bitcoin address, the victim may receive the decryption key. However, there is no guarantee the decryption key will be delivered as promised.

Recording Key Strokes

- Cybercriminals can insert or email you malware called **keyloggers** that can record what you're typing onto your computer. The data is then passed back to the hackers and used to access sensitive data. This can happen at your place of employment, or on your personal computer.
- When this happens, they record everything you are typing. This can include credit card numbers, passwords and sensitive information you might enter into a database like names, health data or anything else.

Phishing:

- Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.

Malware or Virus:

- Malware or viruses can be sent to people with the goal of wiping their computer.

Distributed Denial of Service (DDoS):

- A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

Data Linkage and Profiling

Data Linkage:

Data linking is the process of joining datasets together so that we can make as much use as possible of the information that they hold.

Data Profiling:

Data profiling helps you discover, understand and organize your data.

Data profiling techniques or processes used today fall into three major categories:

- Structure discovery
- Content discovery
- Relationship discovery.

- **Structure discovery**, also known as structure analysis, validates that the data that you have is consistent and formatted correctly.

- **Content discovery** is the process of looking more closely into the individual elements of the database to check data quality. This can help you find areas that contain null values or values that are incorrect or ambiguous.

- **Relationship discovery** involves discovering what data is in use and trying to gain a better understanding of the connections between the data sets.

There are four general methods bywhich data profiling tools help accomplish better data quality:

- Column profiling scans through a table and counts the number of times each value shows up within each column. This method can be useful to find frequency distribution and patterns within a column of data.
- Cross-column profiling is made up of two processes: keyanalysis and dependency analysis.
    - Key analysis examines collections of attribute values by scouting for a possible primary key.
    - Dependency analysis is a more complex process that determines whether there are relationships or structures embedded in a data set.
    - Both techniques help analyze dependencies among data attributes within the same table.

- **Cross-table profiling** uses foreign key analysis, which is the identification of orphaned records and determination of semantic and syntactic differences, to examine the relationships of column sets in different tables.

  This can help cut down on redundancy but also identify data value sets that could be mapped together.
- Finally, **data rule validation** uses data profiling in a proactive manner to verify that data instances and data sets conform with predefined rules. This process helps find ways to improve data quality and can be achieved either through batch validation or an ongoing validation service.

Privacy policies and their specifications

- **Privacy Policy:**

A privacy policy is a legal document that discloses the way a party gathers, uses, discloses, and manages a customer or client's data. It fulfils a legal requirement to protect a customer or client's privacy.

- Such privacy policy must provide the following:
    1. clearly and easily accessible statements of its practices and policies;
    2. clearly state the type of personal and sensitive personal data or information collected by the business;
    3. purpose of collection and usage of such information;
    4. about disclosure of information including sensitive personal data or information collected; and
    5. Reasonable security practices and procedures adopted by it.

- **Elements of a privacy policy:**

The following are the main elements which shall be consisted of a privacy policy, are as follows:

- Consent: The most crucial component of a privacy policy is 'consent'.
- Purpose of information collected.
- Disclosure of information.
- Security practices

Privacy policy languages

- Privacy policy languages can help with several stages involved in managing privacy policies (writing, reviewing, testing, approving, issuing, combining, analyzing, modifying, withdrawing, retrieving and enforcing policy).
- Privacy policy languages were designed to express the privacy controls that both organizations and users want to express.
- Most of the privacy policy languages were designed for specific purposes with specific features and characteristics.
- Most of the initiatives for designing these languages have occurred in the last ten years.
- In 1997, the World Wide Web Consortium (W3C) began development of the Platform for Privacy Preferences (P3P) to express website privacy policies in machine-readable format.
- A P3P Preference Exchange Language (APPEL) was also designed by W3C in 1997 to express an individual's privacy preferences, to query the data represented by P3P, and to make decisions accordingly.
- CPExchange (Customer Profile Exchange) was developed in 2000 to facilitate business-to-business communication about privacy policies.
- Later, the industry felt the need for languages to express the internal privacy policies of the organizations themselves.
- With that goal IBM designed the Enterprise Privacy Authorization Language (EPAL) in 2003.
- During the same period a consortium of organizations joined to design the eXtensible Access Control Markup Language (XACML) for expressing both privacy and security policies in a machine readable format.
- There were other initiatives such as DPAL and XPref in 2003 and 2004. Advances in technology and the rapid use of pervasive computing

Privacy policy languages are expected to be fairly simple and small. Therefore, they have been designed as light-weight XML markup languages. These privacy policy languages are not expected to perform high-level mathematical operations or complicated flow controls.

Privacy in different domains

- Medical privacy or health privacy is the practice of maintaining the security and confidentiality of patient records.
- It involves both the conversational discretion of health care providers and the security of medical records.
- The terms can also refer to the physical privacy of patients from other patients and providers while in a medical facility, and to modesty in medical settings.
- Modern concerns include the degree of disclosure to insurance companies, employers, and other third parties.
- The advent of electronic medical records (EMR) and patient care management systems (PCMS) have raised new concerns about privacy, balanced with efforts to reduce duplication of services and medical errors.

Cybercrime: Examples and Mini-Cases

Examples of Basic Cyber Crimes

- Stolen credit card information.
- Hacking into a government website
- Theft of user accounts.
- Compromised IoT devices.
- Loss of control and access to content.
- Phishing campaigns.
- Individual.
- Property.

Top 5 cyber crimes in India

- Phishing Scams.
- Website Spoofing.
- Ransomware.
- Malware.
- IOT Hacking.

The 2019's Biggest Cyber Attacks in India

1. Cyber criminals have adapted advanced cyber attack techniques for their targeted end-users. Variousbusiness sectors and geographical locations have faced recent cyber attacks in India.
Cosmos Bank Cyber Attack in Pune

2. A recent cyber attack in India in 2018 was deployed on Cosmos Bank in Pune. This daring attack shook the whole banking sector of India when hackers siphoned off Rs. 94.42 crores from Cosmos Cooperative Bank Ltd. in Pune.
Cosmos Bank Cyber Attack

3. Hackers hacked into the bank's ATM server and took details of many visas and rupee debit cardholders. Money was wiped off while hacker gangs from around 28 countries immediately withdrew the amount as soon as they were informed.
ATM System Hacked

4.Around mid-2018, Canara bank ATM servers were targeted in a cyber attack. Almost 20 lakh rupees were wiped off from various bank accounts. A count of 50 victims was estimated and according to the sources, cyber attackers held ATM details of more than 300 users. Hackers used skimming devices to steal information from debit cardholders. Transactions made from stolen details amounted from Rs. 10,000 to Rs. 40,000.

UIDAI Aadhaar Software Hacked

5. 2018 started with a massive data breach of personal records of 1.1 Billion Indian Aadhaar cardholders. UIDAI revealed that around 210 Indian Government websites had leaked the Aadhaar details of people online.

Aadhaar Software Hacked

Aadhaar Software Hacked

6.Data leaked included Aadhaar, PAN and mobile numbers, bank account numbers, IFSC codes and mostly every personal information of all individual cardholders. If it wasn't enough shocking, anonymous sellers were selling Aadhaar information of any person for Rs. 500 over Whatsapp. Also, one could get any person's Aadhaar car printout by paying an extra amount of Rs.300.

Hack Attack on Indian Healthcare Websites

7.Indian-based healthcare websites became a victim of cyber attack recently in 2019. As stated by US-based cyber security firms, hackers broke in and invaded a leading India-based healthcare website. The hacker stole 68 lakh records of patients as well as doctors.

SIM Swap Scam

8.Two hackers from Navi Mumbai were arrested for transferring 4 crore rupees from numerous bank accounts in August 2018. They illegally transferred money from the bank accounts of many individuals. By fraudulently gaining SIM card information, both attackers blocked individuals' SIM cards and with the help of fake document posts, they carried out transactions via online banking. They also tried to hack accounts of various targeted companies.

9. Aforesaid stats and events of the latest cyber attacks in India are the wake-up call for all those individuals and companies who are still vulnerable to cyber threats. It is very essential for organizations to implement cyber security measures and follow the below-mentioned security guidelines.

Cyber Security Measures for Organizations to Prevent Cyber Attacks

- Educate employees on the emerging cyber attacks with security awareness training. 2.Keep all software and systems updated from time to time with the latest security patches.
- Implement email authentication protocols such as DMARC, DKIM and SPF to secure your emaildomain from email-based cyber attacks.
- Get regular Vulnerability Assessment and Penetration Testing to patch and remove the existingvulnerabilities in the network and web application.
- Limit employee access to sensitive data or confidential information and limit their authority to installthe software.
- Use highly strong passwords for accounts and make sure to update them at long intervals.Avoid the practice of openly password sharing at work.