MALLA REDDY COLLEGE OF ENGINEERING & TECHNOLOGY

MRCET CAMPUS

(AUTONOMOUS INSTITUTION – UGC, GOVT. OF INDIA)

Department of CSE

(Emerging Technologies)

(Cyber Security)

B.TECH(R-22 Regulation)

(III YEAR – I SEM)

(2023-24)

CYBER SECURITY

(R22A6202)

LECTURE NOTES

Prepared by

Mrs. V. Divya (Assistant Professor)

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

Department of Computer Science and Engineering

Vision

- "To be at the forefront of Emerging Technologies and to evolve as a Centre of Excellence in Research, Learning and Consultancy to foster the students into globally competent professionals useful to the Society."

Mission

The department of CSE (Emerging Technologies) is committed to:

- To offer highest Professional and Academic Standards in terms of Personal growth and satisfaction.
- Make the society as the hub of emerging technologies and thereby capture opportunities in new age technologies.
- To create a benchmark in the areas of Research, Education and Public Outreach.
- To provide students a platform where independent learning and scientific study are encouraged with emphasis on latest engineering techniques.

QUALITY POLICY

- To pursue continual improvement of teaching learning process of Undergraduate and Post Graduate programs in Engineering & Management vigorously.
- To provide state of art infrastructure and expertise to impart the quality education and research environment to students for a complete learning experiences.
- Developing students with a disciplined and integrated personality.
- To offer quality relevant and cost effective programmers to produce engineers as per requirements of the industry need.

For more information: www.mrcet.ac.in

INDEX

MALLA REDDY COLLEGE OF ENGINEERING AND TECHNOLOGY

III Year B.Tech II Sem

L	T/P/D	C
3	-/-/-	3

(R20A6202) CYBER SECURITY

Course objectives:

- To understand various types of cyber-attacks and cyber-crimes
- To learn threats and risks within context of the cyber security
- To have an overview of the cyber laws & concepts of cyber forensics
- To study the defensive techniques against these attacks

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, 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.

Cyber Crime and Cyber Terrorism: Introduction, Intellectual Property in the Cyber Space, The ethical dimensions of Cybercrimes in 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 in different domains- medical, financial, etc

Cyber Crime Case studies:

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

TEXT BOOKS:

1. Nina Godbole and SunitBelpure, Cyber Security Understanding
2. CyberCrimes, Computer Forensics and Legal Perspectives, Wiley
3. B.B.Gupta,D.P.Agrawal,HaoxiangWang,ComputerandCyberSecurity:Princip le s, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335,2018.

REFERENCES:

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

Course Outcomes:

The students will be able to:

1. Analyze cyber-attacks, types of cybercrimes, cyber laws and also how to protect them self and ultimately the entire Internet community from such attacks.
2. Interpret and forensically investigate security incidents
3. Apply policies and procedures to manage Privacy issues
4. Design and develop secure software modules

z

UNIT-I

INTRODUCTION TO CYBER SECURITY

Cyber Security Introduction - Cyber Security Basics:

Cyber security is the most concerned matter as cyber threats and attacks are overgrowing. Attackers are now using more sophisticated techniques to target the systems. Individuals, small-scale businesses or large organization, are all being impacted. So, all these firms whether IT or non-IT firms have understood the importance of Cyber Security and focusing on adopting all possible measures to deal with cyber threats.

What is cyber security?

"Cyber security is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc."

OR

Cyber security is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

- The term cyber security refers to techniques and practices designed to protect digital data.
- The data that is stored, transmitted or used on an information system.

OR

Cyber security is the protection of Internet-connected systems, including hardware, software, and data from cyber attacks.

It is made up of two words one is cyber and other is security.

- Cyber is related to the technology which contains systems, network and programs or data.
- Whereas security related to the protection which includes systems security, network security and application and information security.

Why is cyber security important?

Listed below are the reasons why cyber security is so important in what's become a predominant digital world:

- Cyber attacks can be extremely expensive for businesses to endure.
- In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage.
- Cyber-attacks these days are becoming progressively destructive. Cybercriminals are using more sophisticated ways to initiate cyber attacks.

- Regulations such as GDPR are forcing organizations into taking better care of the personal data they hold.

  Because of the above reasons, cyber security has become an important part of the business and the focus now is on developing appropriate response plans that minimize the damage in the event of a cyber attack.

  But, an organization or an individual can develop a proper response plan only when he has a good grip on cyber security fundamentals.

Cyber security Fundamentals – Confidentiality:

Confidentiality is about preventing the disclosure of data to unauthorized parties.

It also means trying to keep the identity of authorized parties involved in sharing and holding data private and anonymous.

Often confidentiality is compromised by cracking poorly encrypted data, Man-in-the-middle (MITM) attacks, disclosing sensitive data.

Standard measures to establish confidentiality include:

- Data encryption
- Two-factor authentication
- Biometric verification
- Security tokens

Integrity

Integrity refers to protecting information from being modified by unauthorized parties.

Standard measures to guarantee integrity include:

- Cryptographic checksums
- Using file permissions
- Uninterrupted power supplies
- Data backups

Availability

Availability is making sure that authorized parties are able to access the information when needed.

Standard measures to guarantee availability include:

- Backing up data to external drives
- Implementing firewalls
- Having backup power supplies
- Data redundancy

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 trustworthy entity 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-

1. 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.

2. 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.

3. 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.

4. Backdoors

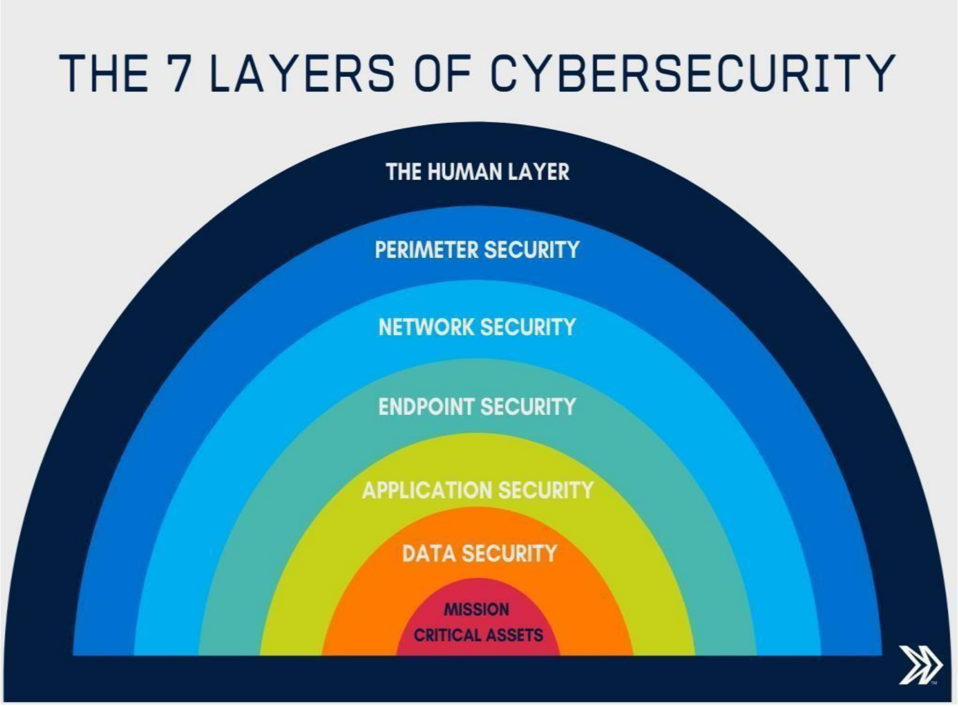
It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

5. 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.

Layers of security:

The 7 layers of cyber security should centre on the mission critical assets you are seeking to protect.



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

Vulnerability, threat, Harmful acts

As the recent epidemic of data breaches illustrates, no system is immune to attacks. Any company that manages, transmits, stores, or otherwise handles data has to institute and enforce mechanisms to monitor their cyber environment, identify vulnerabilities, and close upsecurity holes as quickly as possible.
Before identifying specific dangers to modern data systems, it is crucial to understand the distinction between cyber threats and vulnerabilities.

Cyber threats are security incidents or circumstances with the potential to have a negative outcome for your network or other data management systems.
Examples of common types of security threats include **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 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 include but are not limited to SQL injections, server misconfigurations, cross-site scripting, and transmitting sensitive data in a non-encrypted plain text format.
When threat probability is multiplied by the potential loss that may result, cyber security experts, refer to this as a risk.

Security Vulnerabilities, Threats And Attacks –

Categories of vulnerabilities

- Corrupted (Loss of integrity)
- Leaky(Loss of confidentiality)

- Unavailable or very slow (Loss of availability)

– Threats represent potential security harm to an asset when vulnerabilities are exploited

- Attacks are threats that have been carried out

    - Passive – Make use of information from the system without affecting system resources
    - Active – Alter system resources or affect operation
    - Insider – Initiated by an entity inside the organization
    - Outsider – Initiated from outside the perimeter

Internet governance – challenges and constraints:

- Internet governance is the development and application of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet.
- Internet governance should not be confused with e-governance, which refers to governments' use of technology to carry out their governing duties.
- No one person, company, organization or government runs the Internet.
- It is a globally distributed network comprising many voluntarily interconnected autonomous networks.
- It operates without a central governing body with each constituent network setting and enforcing its own policies.
- Its governance is conducted by a decentralized and international multi stakeholder network of interconnected autonomous groups drawing from civil society, the private sector, governments, the academic and research communities and national and international organizations.
- They work cooperatively from their respective roles to create shared policies and standards that maintain the Internet's global interoperability for the public.
- Law professor Yochai Benkler developed a conceptualization of Internet governance by the idea of three "layers" of governance:
    1. Physical infrastructure layer (through which information travels)
    2. Code or logical layer (controls the infrastructure)
    3. Content layer (contains the information signaled through the network)

Challenges:

1. Resource and Infrastructure Challenges
2. Research and Innovation Challenges
3. Fair Representation and Policy Formulation
4. Policy Participation Challenges
5. Information Mapping Challenges
6. Jurisdiction Issue and Challenges
7. Accountability Challenges
8. Sovereignty Issue and Challenges (Supreme power or Authority)
9. IDN Domain Names
10. Multi stakeholder
11. Data protection
12. Cyber Stalking (harassing)
13. Security
14. Unification Challenges

Constraints:

1. Funding
2. Regulatory
3. Coordination
4. Collaboration Barriers
5. Right to privacy
6. Management of critical Internet resources.

Computer criminals

Computer criminals have access to enormous amounts of hardware, software, and data; they have the potential to cripple much of effective business and government throughout the world. In a sense, the purpose of computer security is to prevent these criminals from doing damage.

We say **computer crime** is any crime involving a computer or aided by the use of one. Although this definition is admittedly broad, it allows us to consider ways to protect ourselves, our businesses, and our communities against those who use computers maliciously.

One approach to prevention or moderation is to understand who commits these crimes and why. Many studies have attempted to determine the characteristics of computer criminals. By studying those who have already used computers to commit crimes, we may be able in the future to spot likely criminals and prevent the crimes from occurring.

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

It's crucial in today's world for people to protect their sensitive, private information from unauthorized access.
Protecting confidentiality is dependent on being able to define and enforce certain access levels for information.

In some cases, doing this involves separating information into various collections that are organized by who needs access to the information and how sensitive that information actually is - i.e. the amount of damage suffered if the confidentiality was breached.
Some of the most common means used to manage confidentiality include access control lists, volume and file encryption, and Unix file permissions.

Integrity

Data integrity is what the "I" in CIA Triad stands for. This is an essential component of the CIA Triad and designed to protect data from deletion or modification For many unauthorized party, and it ensures that when an authorized person makes a change that should not have been made the damage can be reversed.

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.

Understanding the CIA triad

The CIA Triad is all about information. While this is considered the core factor of the majority of IT security, it promotes a limited view of the security that ignores other important factors.

For example, even though availability may serve to make sure you don't lose access to resources needed to provide information when it is needed, thinking about information security in itself doesn't guarantee that someone else hasn't used your hardware resources without authorization.

It's important to understand what the CIA Triad is, how it is used to plan and also to implement a quality security policy while understanding the various principles behind it. It's also important to understand the limitations it presents. When you are informed, you can utilize the CIA Triad for what it has to offer and avoid the consequences that may come along by not understanding it.

Assets and Threat

What is an Asset: 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

What is a threat: 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.

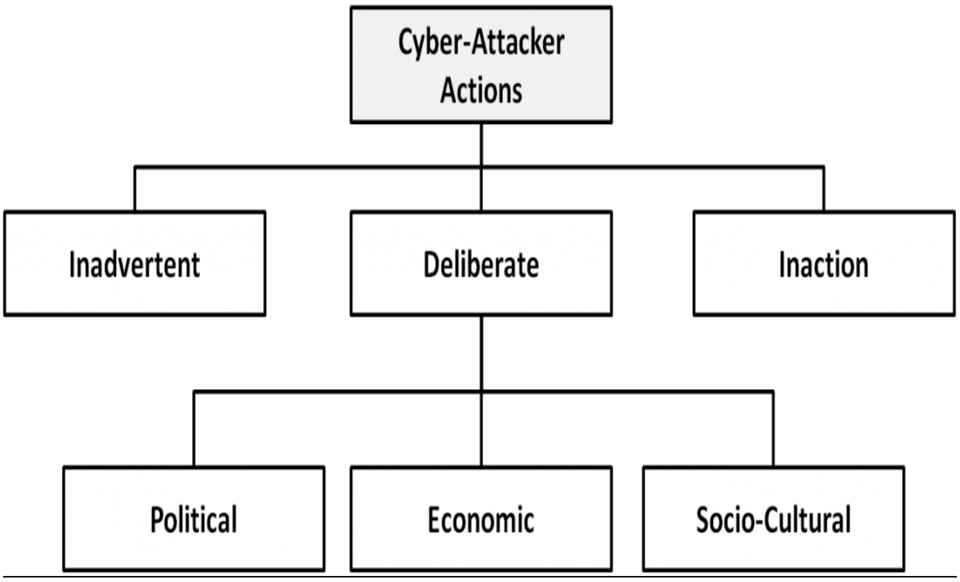
Threats can be categorized as circumstances that compromise the confidentiality, integrity or availability of an asset, and can either be intentional or accidental.

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 of motivation.

1. ***Political motivations:*** examples include destroying, disrupting, or taking control of targets; espionage; and making political statements, protests, or retaliatory actions.
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 publicity or ego gratification.



Types of cyber-attacker actions and their motivations when deliberate

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 modify the 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 canbe 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's knowledge or approval. It can be verydifficult to remove and very damaging. Common malware examples are listed in the following table:

Attack	Characteristics
Virus	A *virus* is a programthat attempts to damage a computer system and replicate itselfto other computer systems. A virus: Requires a host to replicate and usually attaches itself to a host file or ahard drive sector. Replicates each time the host is used. Often focuses on destruction or corruption of data. Usually attaches to files with execution capabilities such as .doc, .exe, and .bat extensions. Often distributes via e-mail. Many viruses can e-mail themselves toeveryone 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 Trojanhorse 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 backdoorfunctions 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 aspecific example of an asynchronous attack. A trigger activity may be a specific date and time, the launching of aspecific program, or the processing of a specific type of activity. Logic bombs do not self-replicate.

Hardware Attacks:

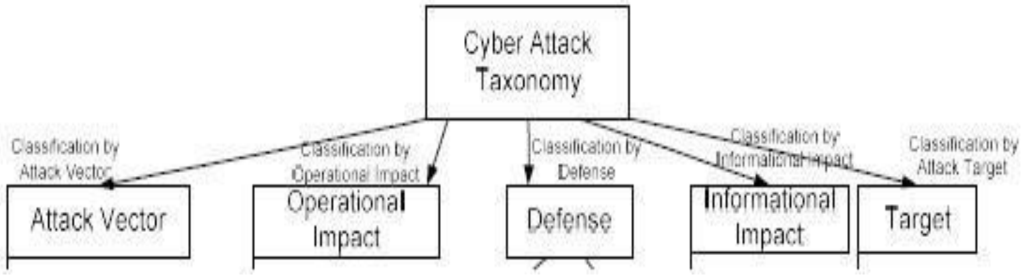
Common hardware attacks include:

- 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 behaviour
- 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 thosemade to gain malicious access to systems.

Taxonomy of Various Attacks:

- Cyber attacks have greatly increased over the years, where the attackers have progressively improved in devising attacks towards a specific target.
- Attacks are becoming more sophisticated and possess the ability to spread in a matter of seconds.
- It is essential to provide tools necessary in detecting, classifying, and defending from various types of attacks.

- To aid in identifying and defending against cyber attacks a taxonomy is required.
- There is a cyber attack taxonomy called AVOIDIT (Attack Vector, Operational Impact, Defense, Information Impact, and Target).
- This will have five major classifiers to characterize the nature of an attack, which are classification by attack vector, classification by attack target, classification by operational impact, classification by informational impact, and classification by defense.


Cyber Attack Taxonomy
Classification by Attack Vector
Classification by Operational Impact
Classification by Defense
Classification by Informational Impact
Classification by Attack Target
Attack Vector
Operational Impact
Defense
Informational Impact
Target

1. **Classification by Attack Vector**: An attack vector is defined as a path by which an attacker can gain access to a host
2. **Classification by Operational Impact**: It provides a mutually exclusive list of operational impacts that can be categorized and concisely presented to the public.
3. **Classification by Defense**:
4. Here several defending strategies are employed against pre- and post- attacks.
5. Mitigation and remediation will be included
6. **Classification by Informational Impact**:
7. An attack on a targeted system has potential to impact sensitive information in various ways.
8. In this section an attacks impact will be classified.
9. **Classification by Attack Target:** Various attacks target a variety of hosts, leaving the defender unknowingly susceptible to the next attack.

IP Spoofing:

- Spoofing is a specific type of cyber-attack in which someone attempts to use a computer, device, or network to trick other computer networks by masquerading as a legitimate entity.
- It's one of many tools hackers use to gain access to computers to mine them for sensitive data, turn them into zombies (computers taken over for malicious use), or launch Denial-of-Service (DoS) attacks.
- There are several types of spoofing attacks; IP spoofing is the most common one.

How spoofing works:

- The data transmitted over the internet is first broken into multiple packets, and those packets are transmitted independently and reassembled at the end.
- Each packet has an IP (Internet Protocol) header that contains information about the packet, including the source IP address and the destination IP address.

- In IP spoofing, a hacker uses tools to modify the source address in the packet header to make the receiving computer system think the packet is from a trusted source, such as another computer on a legitimate network, and accept it. Because this occurs at the network level, there are no external signs of tampering.

Methods of Defense:
Five basic approaches to defense of computing systems

1. Prevent attack:- Block attack / Close vulnerability
2. Deter attack:-Make attack harder (can't make it impossible?)
3. Deflect attack:- Make another target more attractive than this target
4. Detect attack:- During or after
5. Recover from attack

The controls or counter measures are:

❖ The Different Controls or counter measures are

1. Encryption:- In Encryption we take data in normal form i.e unscrambled state, also called as clear text, and transform them into encrypted form, so that it will not understood by the outsiders. The transformed data are called encrypted text or cipher text.

2. Software controls:- Software/program controls include:
   - OS and network controls E.g. Logs/firewalls, OS/net virus scans, recorders
   - Independent control programs E.g. password checker, virus scanner, IDS (intrusion detection system)
   - Internal program controls E.g. read/write controls in DBMSs
   - Development controls E.g. quality standards followed by developers including testing.

3. Hardware controls:- Numerous hardware devices have been created to assist in providing computer security. These devices include a variety of means, such as

- Hardware or smart card implementations of encryption
- Locks or cables limiting access or deterring theft
- Devices to verify users' identities
- Firewalls
- Intrusion detection systems
- Circuit boards that control access to storage media

4. Policies and procedures:-

- Policy: What is allowed /what is not allowed.
- Procedure: How you enforce or implement the policy.
- Sometimes, we can rely on agreed procedures or policies among users rather than enforcing security through hardware or software means.
- Standard rules (legal, ethical and regulations etc.) and their implementation should be established)

5. Physical controls:-

- Physical controls are the easiest, most effective, and least expensive controls.
- Physical controls include locks on doors, guards at entry points, backup copies of important software and data, and physical site planning that reduces the risk of

natural disasters.

Security Models:

- A security model is a computer model which is used to identify and impose security policies.
- A security model is a framework in which a security policy is developed.
- The development of this security policy is related to a particular setting or instance of a policy for example, a security policy based upon authentication.
- A security model thus intended to abstract the security policy and handle its complexity, represent the secure states of a system in which it may evolve.
- A security model verifies the consistency of the security policy, and it will detect and resolve possible conflicts.

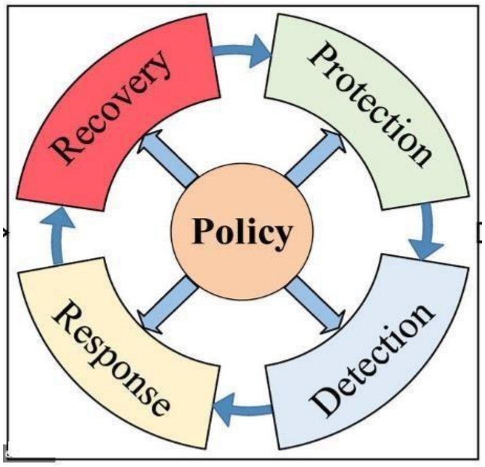


Fig. Security Model

Risk Management:

- Cyber risk management is the process of identifying, analyzing, evaluating and addressing your organization’s cyber security threats.

- The first part of any cyber risk management programme is a cyber risk assessment. This will give you a snapshot of the threats that might compromise your organization’s cyber security and how severe they are.

The cyber risk management process:-

- Although specific methodologies vary, a risk management programme typically follows these steps:

  1) Identify the risks that might compromise your cyber security, This usually involves in identifying cyber security vulnerabilities in your system and the threats that might exploit them.

  2) Analyze the severity of each risk by assessing how likely it is to occur, and how significant the impact might be if it does.

  3) Evaluate how each risk fits within your risk appetite (your predetermined level of acceptable risk).

4) Prioritize the risks.

5) Decide how to respond to each risk. There are generally four options:

i. Treat – modify the likelihood and/or impact of the risk, typically by implementing security controls.

ii. Tolerate – make an active decision to retain the risk (e.g. because it falls within the established risk acceptance criteria).

iii. Terminate – avoid the risk entirely by ending or completely changing the activity causing the risk.

iv. Transfer – share the risk with another party, usually by outsourcing or taking out insurance.

6) Since cyber risk management is a continual process, monitor your risks to make sure they are still acceptable, review your controls to make sure they are still fit for purpose, and make changes as required.

Note: - Remember that your risks are continually changing as the cyber threat landscape evolves, and your systems and activities change.

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 activity that either targets or uses a computer, a computer networkor a networked device. Cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals 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 vulnerablenetworks, web site defacing, Denial-of-service attacks, or terroristic threats made via electronic communication.

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 securityof 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 specificenvironment.

Need of Security policies-

- It increases efficiency.
- It upholds discipline and accountability
- It can make or break a business deal
- It helps to educate employees on security literacy

There are some important cyber security policy recommendations described 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 of viruses and security risks by using 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 peripheral devices 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.

Comprehensive Cyber Security Policy

- Security policies are a formal set of rules which is issued by an organization to ensure that the users who are authorized to access company technology and information assets comply with rules and guidelines related to the security of information.
- It is a written document in the organization which is responsible for how to protect the organizations from threats and how to handles them when they will occur.
- 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.
- A cyber security policy sets the standards of behavior for activities such as the encryption of email attachments and restrictions on the u
se of social media.
- Cyber security policies are important because cyber attacks and data breaches are potentially costly.
- The important three principles of cyber security policies are confidentiality, integrity and availability.
- Comprehensive cyber security practices usually include items like:
- Threat risk analysis
- System vulnerability analysis
- Impact assessments
- Security environment analysis

Some important cyber security policies recommendations describe below-

- Virus and Spyware Protection policy:-This policy provides the following protection
  - It helps to detect, removes, and repairs the side effects of viruses and security risks
- By using signatures.
  - It helps to detect the threats in the files which the users try to download by using
- Reputation data from Download Insight.
- It helps to detect the applications that exhibit suspicious behaviour by using SONAR
- Heuristics and reputation data.
- Firewall Policy:- This policy provides the following protection:
  - It blocks the unauthorized users from accessing the systems and networks that connect
- To the Internet.
  - It detects the attacks by cybercriminals.
  - It 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.
  - It checks the contents of one or more data packages and detects malware which is coming through legal ways.
- Live Update policy:- This policy can be categorized into two types one is Live Update Content policy, and another is Live Update Setting Policy.
  - The Live Update policy contains the setting which determines when and how client computers download the content updates from Live Update.
  - We can define the computer that clients contact to check for updates and schedule when
- And how often clients computer check for updates.

- Application and Device Control:- This policy protects a system's resources from applications and manages the peripheral devices that can attach to a system.
- Exceptions policy:- This policy provides the ability to exclude applications and processes from detection by the virus and spyware scans.
- Host Integrity policy:-This policy provides the ability to define, enforce, and restore the security of client computers to keep enterprise networks and data secure. This policy requires that the client system must have installed antivirus

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 technology devices and networks.

With the benefits carried by the technological advancements, the cyberspace today hasbecome 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 cyber security:

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 hasbeen 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 from the 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 primaryrelevant section of the IPC covers cyber frauds:

Forgery (Section 464)

Forgery pre-planned for cheating (Section 468)

False documentation (Section 465)

Presenting a forged document as genuine (Section 471)

Reputation damage (Section 469)

Companies Act of 2013

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 cyber security diligence. The Companies (Management and Administration) Rules, 2014 prescribes strict guidelines confirming the cyber security obligations and responsibilities upon the company directors and leaders.

NIST Compliance

The Cyber security Framework (NCFS), authorized by the National Institute of Standards and Technology (NIST), offers a harmonized approach to cyber security as the most reliable globalcertifying body.

NIST Cyber security 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 cyber security 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 cyber security ROI Addresses regulatory and contractual obligations Supports the wider information security program By combining the NIST CSF framework with ISO/IEC 27001 – cyber security risk management becomes simplified. It also makes communication easier throughout the organization and across the supply chains via a common cyber security 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 cyber land - can bring about online safety and resilience.

Roles of International Law

In various countries, areas of the computing and communication industries are regulated by governmental bodies λ 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 λ There are also limits on the use of encryption and of equipment which may be used to defeat copy protection schemes λ There are laws governing trade on the Internet, taxation, consumer protection, and advertising λ 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 λ 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’ λ The complexity in types and forms of cybercrime increases the difficulty to fight back ⎝ fighting cybercrime calls for international cooperation λ 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 organizations as well as to connect the central government with the state governments 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. Government 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 by 2016 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 cyber attacks. 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 cyber space 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

Ministryof 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 way of conformity assessment (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 recovery actions.

Introduction: Historical Background of 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 3

CYBERCRIMES: MOBILE AND WIRELESS DEVICES

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 University systems, email, banking

Proliferation of mobile and wireless devices:

- People hunched over their smart phones or tablets in cafes, airports, supermarkets and even at bus stops, seemingly oblivious 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.

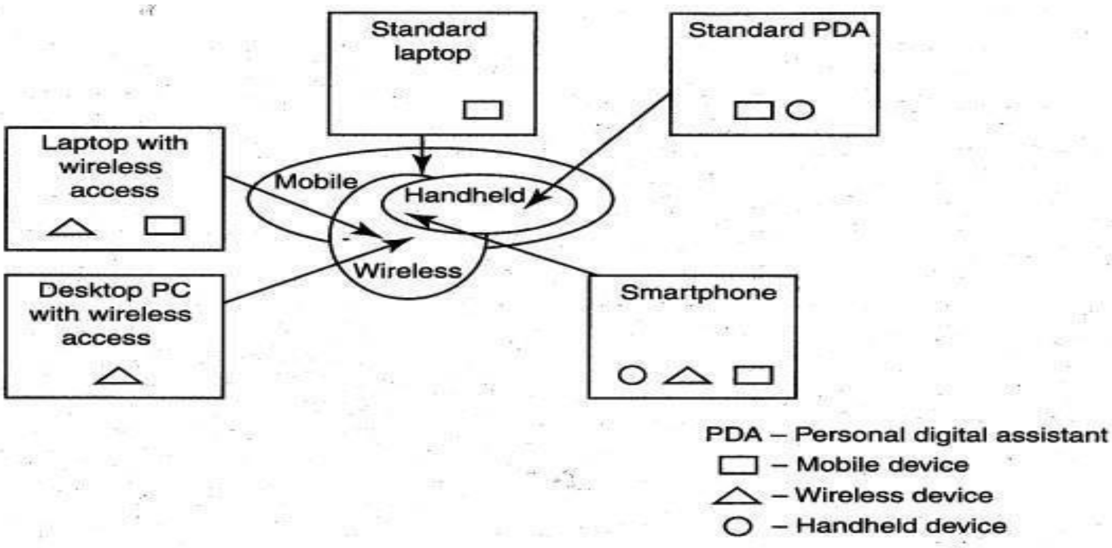


Figure : Mobile, Wireless and hand-held Devices

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 touch screen 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. Ultra mobile (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 Smart phoneshave 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 Pen top 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 plentyof 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.

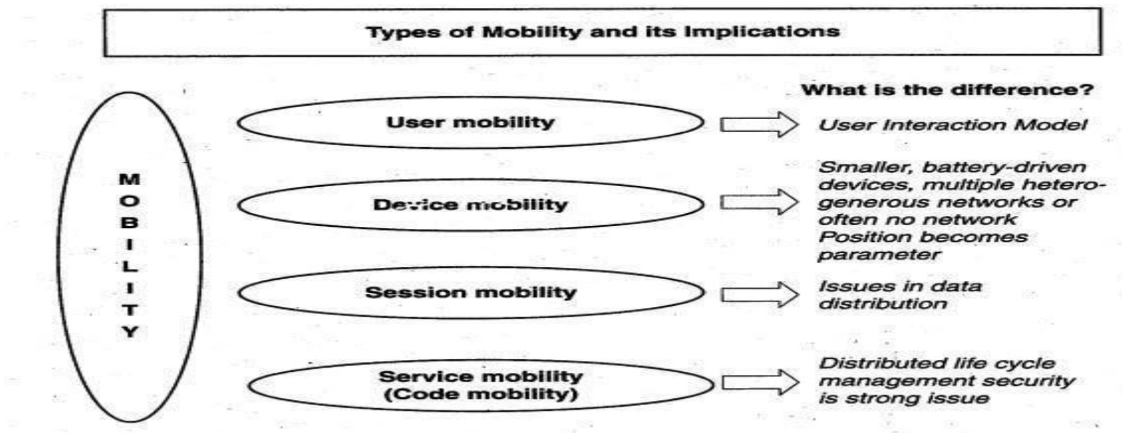

Types of Mobility and its Implications
MOBILITY
What is the difference?
User mobility
User Interaction Model
Device mobility
Smaller, battery-driven devices, multiple hetero-generous networks or often no network Position becomes parameter
Session mobility
Issues in data distribution
Service mobility (Code mobility)
Distributed life cycle management security is strong issue

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 Smart phones, notebook computers or even desktop computers connected to the 3G network.

Popular types of attacks 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, 2.5G, 2G, 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:*** I targets 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 isavailable 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 activity which 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

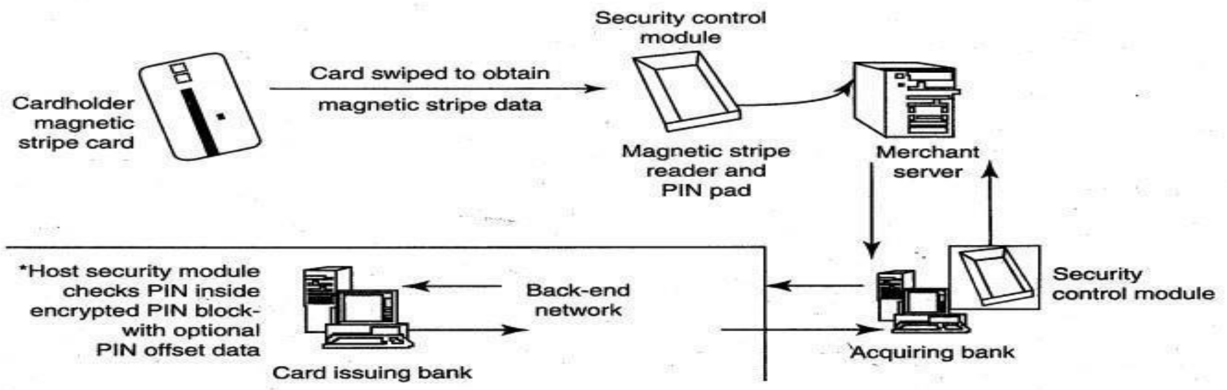

Security control module
Cardholder magnetic stripe card
Card swiped to obtain magnetic stripe data
Magnetic stripe reader and PIN pad
Merchant server
*Host security module checks PIN inside encrypted PIN block- with optional PIN offset data
Back-end network
Card issuing bank
Security control module
Acquiring bank

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 cyber security: 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 tothese cyber security challenges are important in devising appropriate security operating procedure. When people are asked about important in managing a diverse range of mobile devices, they seem 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.

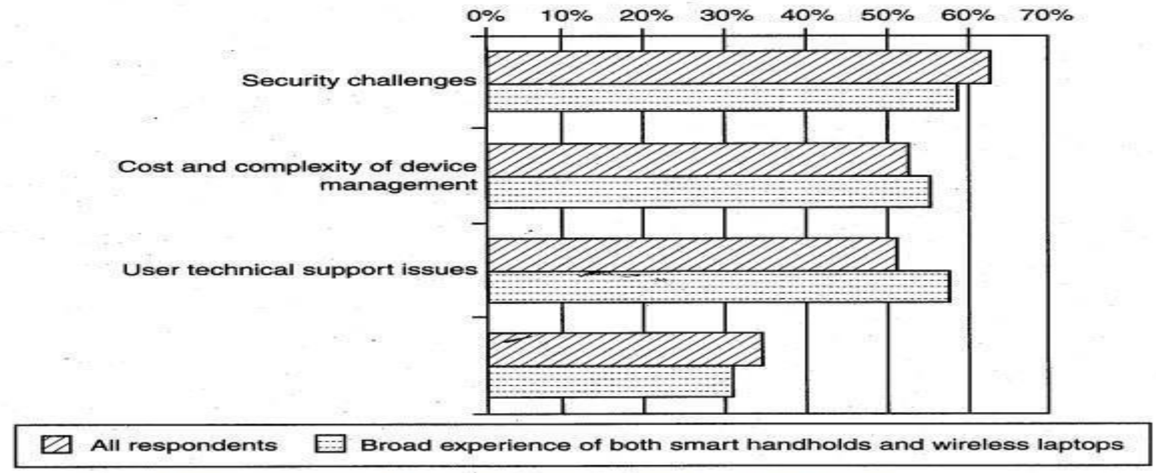


Figure: Important issues for managing mobile devices

Registry Settings for Mobile Devices:

Let us understand the issue of registry settings on mobile devices through an example: Microsoft Active sync 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 security of 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 on mobile 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**

Organizational security Policies and Measures in Mobile Computing Era:

Proliferation of hand-held devices used makes the cyber security issue graver than what we would tend to think. People have grown so used to their hand-held’s 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 regulatory environment.
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.

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 cyber security 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 varietyof 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 toa 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 forthe 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 security guards 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 anti theft 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 handling of removable drives/storage mediums /unnecessary ports.
6. Password protection through appropriate passwords rules and use of strong passwords.
7. Locking down unwanted ports/devices.
8. Regularly installing security patches and updates.
9. Installing antivirus software/firewalls / intrusion detection system (IDSs).
10. Encrypting critical file systems.

UNIT- IV

CYBER SECURITY: ORGANIZATIONAL IMPLICATIONS

Introduction

- Security risks within an organization include - processing of fraudulent transactions, unauthorized access to data & program files, physical theft or damage of equipment.
- Technical innovation and the centralization of data create opportunities for cyber criminals to misappropriate critical information from a single target attack.
- With the online systems allowing its services to become more available, this further multiplies significantly the opportunities to penetrate security measures.

Cost of Cybercrimes and IPR Issues

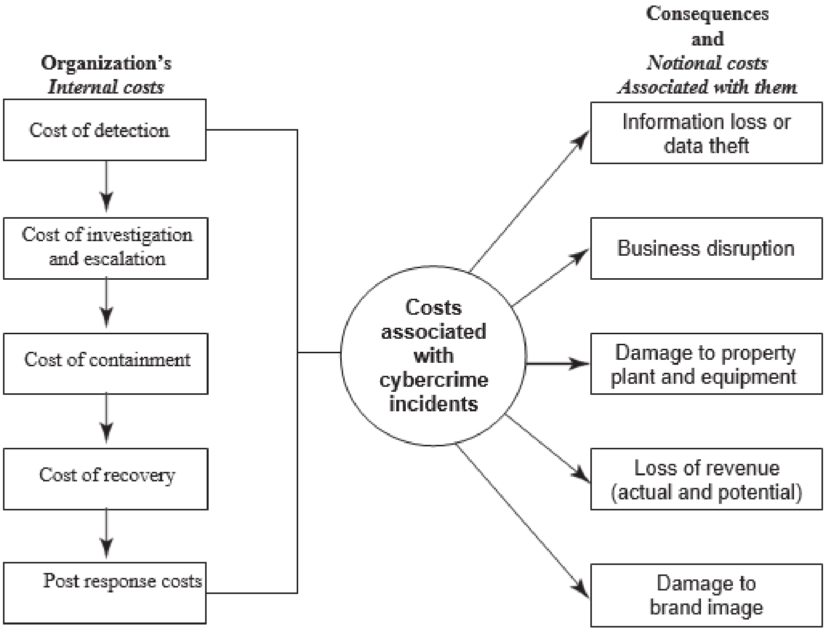

Organization's
Internal costs
Cost of detection
Cost of investigation and escalation
Cost of containment
Cost of recovery
Post response costs
Costs associated with cybercrime incidents
Consequences and Notional costs Associated with them
Information loss or data theft
Business disruption
Damage to property plant and equipment
Loss of revenue (actual and potential)
Damage to brand image

Fig: Cost of cybercrimes.

- 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 are

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

Intellectual property issues in cyber security:-

- Cyber theft of Intellectual Property (IP) is one of them.
- Cyber theft of IP means stealing of copyrights, trade secrets, patents etc., using internet and computers.
- Copyrights and trade secrets are the two forms of I Intellectual Property that is frequently stolen.
    - Intellectual Property Rights Issues:
- The five major challenges faced are
- Patent ever greening prevention
- Subsidies & IPR Issues
- The Product Patents Process
- Protecting traditional knowledge
- Compulsory Licensing & Drug Price Control Order

1. Patent ever greening prevention:-

- One of the most important intellectual property rights issues challenges is the prevention of the ever greening of the patents for multinational companies.
- The term of a granted patent in a jurisdiction that is about to expire, in order to retain royalties from them, by taking out new patents..... This is known as the Ever-greening of a patent.
- As we know, the companies cannot evergreen their patents simply by making minor changes. So, section 3(d) in the Indian Patent Act (IPA) possess as one of the biggest issues with regards to IPR.
- This act bars the grant of patents to new forms of substances....

2. **Subsidies & IPR Issues:**

- The government provides subsidies to people especially farmers to reduce their burden.
- A major form of subsidies includes food subsidy, fertilizer subsidy, education subsidy, etc. However, for the complete implementation of TRIPS agreements (The TRIPS Agreement is a minimum standards agreement, which allows members to provide more extensive protection of intellectual property if they so wish), one needs to reduce or eliminate these subsidies. Thus, the Indian government needs to create a balance between providing subsidies and providing IP rights in India....

3. **The Product Patents Process:**

- A product patent protects a product.
- It offers high protection to the original inventor to reduce the competition for the same product.
- Whereas, a process patent protects the process through which one manufactures the product and not the product.

4. **Protecting traditional knowledge:**

- Traditional knowledge, especially in the field of medicine, is like a gold mine.
- The Indian government is bound to protect the traditional knowledge by not allowing MNC's to get patents on the traditional culture.
- Above all, the government has created a Traditional Knowledge Digital Library (TKDL) to prevent the patenting of traditional knowledge. So, this is one of the intellectual property rights issues in India....

5. **Compulsory licensing & Drug price control order:**

- One of the most important intellectual property rights issues that the government needs to address is the use of compulsory licensing. It's a relaxation available to the developing countries under the TRIPS agreement, something which organizations misuse sometimes. Moreover, under section 84 of the IPA, a company can acquire a compulsory license for "private commercial use" under certain circumstances.
- With the Drug Price Control Order, the company needs to justify the price of the drug with regards to investments. If someone plays foul, then the government has the right to intervene.
- Multinationals are asking the government to revoke this provision. However, the government is not ceding the demands to protect the interest of the masses.

Web Threats for Organizations

- 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.

Overview of Web Threats to Organizations:

- Large number of companies as well as individuals have a connection to the Internet.
- Employees expect to have Internet access at work just like they do 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.

  Some important issues that are to be considered are

  1. Employee Time Wasted on Internet Surfing (People seem to spend approximately 45-60 minutes each working day on personal web surfing at work).
  2. Monitoring and Controlling Employees' Internet Surfing
  3. Keeping Security Patches and Virus Signatures Up to Date
  4. Surviving in the Era of Legal Risks
  5. Bandwidth Wastage Issues
  6. Mobile Workers Pose Security Challenges
  7. Controlling Access to Web Applications
  8. The Bane of Malware
  9. The Need for Protecting Multiple Offices and Locations

Web Threat

- A web threat is any threat that uses the World Wide Web to facilitate cybercrime.
- Web threats use multiple types of malware and fraud, all of which utilize HTTP or HTTPS protocols, but may also employ other protocols and components, such as links in email or malware attachments or on servers that access the Web.
- They benefit cybercriminals by stealing information.
- Web threats pose a broad range of risks, including financial damages, identity theft, loss of confidential information/data, theft of network resources, damaged brand/personal reputation, and erosion of consumer confidence in e-commerce and online banking.
- Web threat has increasing impact on society due to the spread of IT processes.
- Web threats can be divided into two primary categories, based on delivery method – push and pull.
- Push-based threats use spam, phishing, or other fraudulent means to lure a user to a malicious (often spoofed) website which then collects information and/or injects malware. Push attacks use phishing, DNS poisoning (or pharming), and other means to appear to originate from a trusted source.
- In some sort of push-based web threats, malware authors use social engineering such as enticing subject lines those reference holidays, popular personalities, sports, world events and other hot topics to persuade recipients to open the email and follow links to malicious websites or open attachments with malware that accesses the Web.
- Pull-based web threats are often referred to as “drive-by” threats by experts (and more commonly as “drive-by downloads” by journalists and the general public), since they can affect any website visitor.
- Cybercriminals infect legitimate websites, which unknowingly transmit malware to visitors

or alter search results to take users to malicious websites. Upon loading the page, the user's browser passively runs a malware downloader in a hidden HTML frame (IFRAME) without any user interaction.

- The growth of web threats is a result of the popularity of the Web – a relatively unprotected, widely and consistently used medium that is crucial to business productivity, online banking, and e-commerce as well as the everyday lives of people worldwide.

Prevention and detection:

- Conventional approaches have failed to fully protect consumers and businesses from web threats.
- The most viable approach is to implement multi-layered protection—protection in the cloud, at the Internet gateway, across network servers and on the client.

Security and Privacy Implications

- Cyber-security systems, which protect networks and computers against cyber attacks, are becoming common due to increasing threats and government regulation.
- At the same time, the enormous amount of data gathered by cyber-security systems poses a serious threat to the privacy of the people protected by those systems.
- If cybercriminals penetrate into a bank database (this is called as security breach). Your information is exposed and could be sold on the dark web. Your privacy is gone. You could become the victim of cyber fraud and identity theft.
- Privacy protection and cyber security should be thought of as interconnected: as more and more personal information is processed or stored online, privacy protection increasingly relies on effective cyber security implementation by organizations to secure personal data both when it is in transit and at rest.

Privacy Implications;

There are multiple implications, including legal ones, extending to the privacy of personal information held on mobile devices.

Some privacy implications include:

1. Access to personal or corporate email.
2. Access to SMS.
3. Access to images.
4. Access to network (personal, wireless, corporate, VPN).
5. Access to corporate apps and data.
6. Ability to send SMS to premium rated services (e.g., “Toll Fraud”).
7. Privacy threats may be caused by applications that are not necessarily malicious, but gather or use more sensitive information than is necessary to perform their function.
8. Use of location-based services technology such as a global positioning system (GPS).
9. Staff from the outsourcer may act in an unethical way regarding access to privacy-related information.

Note: The Internet never forgets. It's not just what is seen at the time, but also what is archived and recorded by countless services. Just because you delete a tweet doesn't mean it can't be used against you. So Privacy should be considered as a serious issue.

What is security implementation:

- Just think once, what happen if there is no data security - Your files can be copied, altered, or destroyed. Depending on what sorts of files you possess and how important they are to your daily operations, not having cyber security can result in a range of damage ranging from being inconvenienced to shut down completely.
- Security features include: A single security interface for all components.
- The single authentication and authorization mechanism simplifies the security implementation.
- It views and interacts with all components in a consistent manner. System-wide role-based access control.

Social Media Marketing: Security Risks and Perils for Organizations

What is meant by social media marketing:

- The term social media marketing (SMM) refers to the use of social media and social networks to market a company's products and services.
- Social media marketing provides companies with a way to engage with existing customers and reach new ones while allowing them to promote their desired culture, mission, or tone.
- Social media marketing is the use of social media platforms to connect with your audience to build your brand, increase sales, and drive website traffic.

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:

- To be able to reach to a larger target audience in a more spontaneous and instantaneous manner without paying large advertising fees.
- 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.
- To reap other potential revenue benefits and to minimize advertising costs because social media complements other marketing strategies such as a paid advertising campaign.
- To build credibility by participating in relevant product promotion forums and responding to potential customers' questions immediately.
- 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.

The 6 Most Effective Types of Social Media Advertising in 2021

1. Facebook Advertising.
2. Instagram Advertising.
3. Twitter Advertising.
4. Pinterest Advertising.
5. LinkedIn Advertising.
6. Snapchat Advertising.

Security risks and perils for organizations:

Malicious apps, spyware, and viruses have made their way onto social media and into relatedapps as well. While it's not easy to pass viruses through Facebook or LinkedIn, it's easier for hackers to compromise the apps your employees may have on their smart phones that allow them to post to these sites.

1. Data breaches (information stolen incident))have demonstrated weaknesses in social networks for hackers.
2. Attackers use distributed denial-of-service (DDoS) attacks (among other attacks) to compromise the infrastructure systems in your organization. These attacks might result in data exposure or data breach.
3. The challenge comes in phishing and spear phishing.
4. Social media comes with risks of identity theft. Brands with weak user account passwords, customers who download all attachments and those who give confidential details, and others are exposed to risks.
5. The function of CRMs is to identify, acquire, and store customer data for digital marketing. As such, malicious attackers might exploit any vulnerability in the system. Attackers use DDoS attacks, identity theft, data breaches, and malware.
6. Vulnerabilities in E-Commerce systems make it challenging for digital marketers to convert potential customers. Weak links occur in systems security flaws and in identity theft.
7. There are security risks and threats in every aspect of digital marketing. During marketing campaigns, marketers share and parcel data across different systems and platforms.
8. Protecting a system against cyber attacks requires planning and time. Organizations need to identify the risks and where they lie to find the best strategies to safeguard it.

Disadvantages of social media marketing:

1) Not built for business.
2) Negative feedback and tarnish brand.
3) Heavily rely on ads.
4) Low ROI.
5) Time-consuming.
6) Need to stay engaged and active.
7) Difficult to measure.
8) Security and privacy policy issues.

Social Computing and the Associated Challenges for Organizations In Cyber Security

Social computing:

- ❖ Social computing is an area of computer science that is concerned with the intersection of social behavior and computational systems.
- ❖ It is based on creating or recreating social conventions and social contexts through the use of software and technology. Thus, blogs, email, instant messaging, social network services etc…
- ❖ The simplest examples of social computing would include e-mail, discussion forums and instant messenger clients.
- ❖ The most obvious examples would include all the social networks such as Twitter, Facebook and LinkedIn etc. ...
- ❖ Social computing has become a deeply complex and interesting field of research and creativity.
- ❖ Social Computing helps the organizations in many ways like sharing the knowledge among the different users, keeping them up to date about different knowledge and experiences, reducing the interruptions and finding the experts for different purposes and connecting them accordingly.

Issues associated with social computing:-

1) **Misusing Identity:** The attacker impersonates the identity of any user results in misusing identity.
2) **Threats from using 3rd Party Applications:** These applications seek permission from the user to access personal information for all the various games and apps.
3) **Trusting Social Networking Sites Operators:** The contents that user uploads or posts on social networking sites, the information is available with the networking operators. The operators can save account data even after deletion.
4) **Viruses, Phishing Attacks and Malwares:** Viruses and malware often find their way onto your computer through those annoying ads. After gaining access to the network, the attacker can access or steal confidential data by spreading spam mails.
5) **Legal Issues:** Posting contents that are offensive to any individual or community or country. There are legal risks associated with the use of social networking sites like leaking confidential information on sites or invading someone's privacy.
6) **Tracking Users:** It can cause physical security concerns for the user, as the third parties may access the roaming information of the user by collecting the real-time update on the user's location.
7) **Privacy of Data:** Users share their information on social networking sites and can cause privacy braches unless proper security measures are applied.

Risks and Challenges:

1) Phishing Attacks:

- Phishing Attacks: It is a fraudulent action of sending spam emails by imitating to be from any legitimate source.
- Such mails have a strong subject line with attachments like an invoice, job offers, big offers from reputable shipping services or any important mail from higher officials of the company.
- The phishing scam attacks are the most common cyber attacks which aims to steal sensitive data. Like Login credentials, credit card numbers, bank account information and so on.
- To avoid this, you should learn more about phishing email campaigns and its preventive measures. One can also use email filtering technologies to avoid this attack.

2) **Identity Federation Challenges:** It is a technique used to share user credentials across multiple domains. For example, many sites offer users to log in by their Facebook account so that it is more convenient to the user and the user does not have to make multiple accounts across different sites. It may seem convenient but the user does not have the knowledge about on how and to what extent their personal information can be shared among third party applications.

3) **Malwares:** Malwares are the programs that are installed in the user's devices without the knowledge and consent of the user.
a) 'LOL' Virus: This virus spreads through chat function of Facebook. This virus is sent to the user stating "lol" with an attachment. And when the user clicks on the link a malware is downloaded to the user's system. The virus infects the system and spreads through the network gaining access to the user's information.
b) Zeus: This is a Trojan that spreads by clicking on the link. And when a user clicks on the link it scans all the files on the user's system and steals the important information. The specialty of this Trojan is to steal bank credentials of the user.

4) **Click Jacking Attacks:** also called UI redress attacks. Where the Trojan in web pages asks the user to click on the malicious link, and a malware is planted onto the system. This is common in Facebook with the name like jacking that is when a user likes a page, a picture or a video the user is trapped by the attackers. This type of attacks are done to do malicious attack or to make some page popular.

Cybercrime and Cyber terrorism

Introduction: It prohibits unauthorized access to computers and the illegal use of digital information. Internet usage has increased, and so has cyber crimes. There are several stories of cyber crimes in the media today ranging from identity theft, crypto jacking, child pornography, cyber terrorism etc.

There are five main types of cyber terrorism attack which are:
Incursion, destruction , disinformation, denial of service and defacement of web sites. Some of these attacks are more severe than the others and have different objectives.

While the obvious targets might be governments, banks, and utilities (e.g. water, oil, electricity, gas, chemical, and communication infrastructure), as attacks on these have the ability to cause the most economic, political, and physical havoc and damage to the critical national infrastructure. For terrorists, cyber-based attacks have distinct advantages over physical attacks. They can be conducted remotely, anonymously, and relatively cheaply, and they do not require significant investment in weapons, explosives or personnel. The effects can be widespread and profound.

Intellectual property in the cyberspace:

It refers to the possession of thought or design by the one who came up with it. It offers the owner of any inventive design or any form of distinct work some exclusive rights, that make it unlawful to copy or reuse that work without the owner's permission. It is a part of property law.
the different types of intellectual property rights in cyber space
Patent, Copyright, Trademarks, Trade Secrets, Industrial and Layout Designs, Geographical Indications etc. are intellectual property rights. When these rights are violated in cyberspace there are various remedies in law.
The different types of intellectual property rights in cyber space are Patent, Copyright, Trademarks, Trade Secrets, Industrial and Layout Designs, Geographical Indications etc. When these rights are violated in cyberspace there are various remedies in law.

Theethical dimension of cyber crimes in the psychology

It is considered a cyber-crime when the weapon involved in the crime is computers, a network of computers and the internet. It helps aid in several illegal activities from violating one's privacy to trafficking in child pornography and even committing fraud.

Mindset and skills of hackers and other cybercriminals:

Many hackers are intelligent, highly skilled, and they enjoy taking risks. Most successful hackers have backgrounds in computer-related courses and have good social and communication skills that help them manipulate people to provide their essential information.

Some of the most important skills required for ethical hacking professional to be a part of the future of cybersecurity are:

- Networking Skills.
- Computer Skills.
- Linux Skills.
- Programming Skills.
- SQL Skills.
- Hardware Knowledge.
- Knowledge in Reverse Engineering.
- Cryptography.

Different Types of Hackers

- Black Hat. The stereotypical 'hacker' – the kind you hear about on the news. ...
- White Hat. The Yang to the Black Hat's Yin, White Hat hackers are the polar opposite of the Black Hat in every way. ...
- Grey Hat. ...
- Blue Hat. ...
- Red Hat. ...
- Green Hat. ...
- Script Kiddie.

UNIT – V

CYBER SECURITY: ORGANIZATIONAL IMPLICATIONS

Basic Data Privacy Concepts

Data Privacy: -

- Data privacy is centered around how data should be collected, stored, managed, and shared with any third parties, as well as compliance with the applicable privacy laws.
- Data privacy, sometimes also referred to as information 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.
- It is an area of data protection that concerns the proper handling of sensitive data including, personal data and other confidential data such as certain financial data and intellectual property data.
- The fundamentals of data privacy include data confidentiality, data security, limitation in data collection and use, transparency in data usage, and compliance with the appropriate data privacy laws.
- Organizations should use best security practices for protecting sensitive data.
- Data Privacy is not just about the proper handling of data but also about the public expectation of privacy

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.

Elements of data privacy:

Data Privacy or Information privacy encompasses 3 elements:

1. Right of an individual to be left alone and have control over their personal data.
2. Procedures for proper handling, processing, collecting, and sharing of personal data.
3. Compliance with data protection laws.

Data Linking and Profiling

Data linking

- A data link is the means of connecting one location to another for the purpose of transmitting and receiving digital information (data communication). These are governed by a link protocol enabling digital data to be transferred from one location to other location.

There are at least three types of basic data-link configurations that can be conceived of and used:

1. Simplex communications: Most commonly meaning all communications in one direction only.
2. Half-duplex communications: Means communications in both directions, but not both ways simultaneously.
3. Duplex communications: Communications in both directions simultaneously.

Data profiling

- It is the process of reviewing source data, understanding structure, content and interrelationships, and identifying potential for data projects. Ex: data warehouse and business intelligence (DW/BI) projects.
- Data profiling can uncover data quality issues in data sources, and what needs to be corrected in ETL (Extract Transform and Load)
- Data profiling is the process of examining the data available from an existing information source (e.g. a database or a file) and collecting statistics or informative summaries about that data. And assess the risk involved in integrating data in new applications, including the challenges of joins.
- It is the act of monitoring and cleansing data, which is an important tool that can be used by the organizations to make better data decisions.
- Data profiling is an often-visual assessment that uses a toolbox of business rules and analytical algorithms to discover, understand and potentially expose inconsistencies in your data. This knowledge is then used to improve the quality of data.
- The need for data profiling is going to grow.
- Corporate data warehouses must interact with increasingly diverse and large sets of data from different sources like blogs, social media and emerging big data technologies like Hadoop.
- In the industrial world, the Internet of Things introduces a multitude of devices generating data, while organizations can access data from biometrics and human-generated sources like email and electronic medical records.
- Data that isn’t formatted right, standardized or correctly integrated with the rest of the database can cause delays and problems that lead to missed opportunities, confused customers and bad decisions.
- Data profiling helps you to get ahead of these issues. By ensuring that you run a diagnosis and examine the data that you have, you can proactively create a plan to fix many of your data problems and clean up your data warehouse before they can affect your organization.

Different kinds of data profiling techniques.
There are three major categories of data profiling techniques are available:
Structure discovery

- Content discovery
- Relationship discovery.

1. **Structure discovery:**

- It also known as structure analysis.
- It validates whether the data we have is consistent and formatted correctly or not.
- There are several different processes that you can use for this, such as pattern matching. For example, if you have a data set of phone numbers, pattern matching helps you find the valid sets of formats within the data set. Pattern matching also helps you understand whether a field is text- or number-based along with other format-specific information.
- Structure discovery also examines simple basic statistics in the data. By using statistics like the minimum and maximum values, means, medians, modes and standard deviations, you can gain insight into the validity of the data.

2. **Content discovery: -**

- 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.
- The standardization process in content discovery plays a major role in fixing incorrect or

ambiguous problems. For example, finding and correcting your data to fit street addresses into the correct format is an essential part of this step.

- The potential problems that could arise from non-standard data, like being unable to reach customers via mail because the data set includes incorrectly formatted addresses, are costly and can be addressed early in the data management process.

3. Relationship discovery: -

- Relationship discovery involves discovering what data is in use and trying to gain a better understanding of the connections between the data sets.
- This process starts with metadata analysis to determine key relationships between the data and narrows down the connections between specific fields, particularly where the data overlaps.
- This process helps to solve the problems that arise in data warehouse or other data sets when data is not aligned.

Privacy Policies and Their Specifications

- 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 fulfills a legal requirement to protect a customer or client's privacy about disclosure of information including sensitive personal data or information collected.
- Privacy policies typically represent a broader, more generalized treatment, which tend to be more detailed and specific.
- The exact contents of a certain privacy policy will depend upon the applicable law and may need to address requirements across geographical boundaries and legal jurisdictions.
- Most countries have their own legislation and guidelines of who is covered, what information can be collected, and what it can be used for.

A privacy policy must provide the following (elements of a privacy policy)

1. Clearly and easily accessible statements of its practices and policies.
2. Clearly state the type of sensitive personal data or information collection and usage of such information.
3. Clearly state about the disclosure of information collected.
4. About the reasonable security practices and procedures adopted by it.

A privacy policy typically contains sections to address:

1. Scope
2. Type of information (electronic, paper, encrypted?)
3. Who the policy applies to (employees, contractors, vendors?)
4. Policy statement
5. Expected behavior
6. Consequences of non-compliance (failure)
7. Definition of personal information
8. Information classification
9. Protection standards
10. Destruction standards
11. Whom to call for questions and concerns

Privacy Policies Languages

- Privacy policy languages were designed to express the privacy controls that both organizations and users want to express.
- Privacy policies is an essential aspect in the management of customer relationships.

- Organizations express their internal privacy practices as statements in the privacy policies.
- Consumers are able to analyze the organization's stated commitment towards protecting consumers' privacy through these privacy policies.
- Different types of languages are available to represent the human readable policies in more precise and computer compatible formats.
- Most of the privacy policy languages were designed for specific purposes with specific features and characteristics.
- Many privacy languages are available for representing policies, but they tend to use formats convenient to their implementations, and there is no single framework or metric to analyze and evaluate the effectiveness of these languages.
- Some languages are designed to help organizations express their privacy policies in ways that are more amenable to policy enforcement, and some languages are designed to help users define their privacy preferences. These preferences can then be employed to help users make decisions.
- Privacy policy languages are expected to be fairly simple and small.
- These privacy policy languages are not expected to perform high-level mathematical operations or complicated flow controls.

Privacy in Different Domains

- Privacy in medical domain and financial domains etc….
- Confidentiality and privacy are essential to all trusting relationships, such as that between patients and doctors.
- Moreover, in a healthcare context, patient confidentiality and the protection of privacy is the foundation of the doctor-patient relationship.
- Financial privacy laws regulate the manner in which financial institutions handle the nonpublic financial information of consumers.
- In the United States, financial privacy is regulated through laws enacted at the federal and state level.

Cyber Crime Case Studies:

The Indian case of online Gambling:

Gambling in India varies by state; states in India are entitled to formulate their own laws for gambling activities. Some states like Goa have legalised casinos. Common gambling activities like organized betting are restricted except for selective categories including lottery and horse racing. In the 21st century, more people have started making cash bets upon prohibited betting and gambling activities in India. Critics of gambling claim that it leads to crime, corruption, and money laundering. However, proponents of regulated gambling argue that it can be a huge source of revenue for the state. Casinos in Goa contributed Rs. 135 crores to the state revenue in 2013.[1] Recently published research revealed that Maharashtra state supplies the most online casino players in the country.
Casinos now operate in Goa, Daman, and Sikkim.

Legality:
Gambling is a state subject, and only states in India are entitled to formulate laws for gambling activities within their respective states. The Public Gambling Act of 1867 is a central law that prohibits running or being in charge of a public gambling house. The penalty for breaking this law is a fine of ₹200 or imprisonment of up to 3 months. The Act also prohibits visiting gambling houses. A fine of ₹100 or imprisonment of up to one month is the penalty.

Indian law classifies games into two broad categories *viz.* game of skill and game of chance. The Supreme Court of India has held·

The game of Rummy is not a game entirely of chance like the 'three-card' game mentioned in the Madras case to which we were referred. The 'three cards' game which goes under different names such as 'flush', 'brag' etc. is a game of pure chance. Rummy, on the other hand, requires a certain amount of skill because the fall of the cards has to be memorised and the building up of Rummy requires considerable skill in holding and discarding cards. We cannot, therefore, say that the game of Rummy is a game of entire chance. It is mainly and preponderantly a game of skill.

The Information Technology Act 2000 regulates cyber activities in India does not mention the word Gambling or Betting thereby the act was left for interpretation by the Courts which have refused to examine the matter. Further, online gambling is a banned offence in the state of Maharashtra under the "Bombay Wager Act".

Only three states, Goa, Daman and Sikkim, allow casinos. There are two casinos in Sikkim called Casino Sikkim and Casino Mahjong and ten in Goa, of which six are land-based and four are floating casinos that operate on the Mandovi River. The floating casinos in Goa are Casino Deltin Royale, Casino Deltin JAQK, Casino Pride, and Casino Pride 2. While the first two are controlled by the Deltin Group, the latter two are managed by the Pride Group. According to the Goa, Daman and Diu Public Gambling Act, 1976 casinos can be set up only at five-star hotels or offshore vessels with the prior permission of the government. This has led the Deltin Group to open the first land-based Casino in Daman which is open now. News reports also suggest that Visakhapatnam is also being looked on as the next casino destination.

Online

Online gambling is in its infancy in India:

- There are no *federal* laws that prohibits online betting in India
- A few states have made recently explicit laws against online betting
- Ancient regulations like the Public Gambling Act of 1867 are still in place. however there are not any cases on record of Indian players being prosecuted for online betting.

In 2010, Sikkim planned to offer three online gambling licences. By 2022 online gambling is only officially legal in the states of Goa, Daman and Sikkim. Sikkim also permits an online lottery, which takes bets from players throughout India. It was expected that other states would follow Sikkim, thereby opening up a major online gambling market aka **Satta Matka** throughout India.

Even though Indian casinos cannot promote or have sites that promote online gambling games such as casinos, sports betting, and bingo, it is not illegal for non-Indian casino companies (so-called offshore companies) to have sites that focus on Indian players. The only legal requirement is that the offshore casinos have to offer Indian Rupees as a payment method for Indian players. Although this is not accurate anymore since January 2020 as the states Telangana and Andhra Pradesh banned all online gambling for Indians. Anyone breaking this new law will receive up to one year in prison or a fine.

Legalisation.

Despite the existing prohibitive legislations, there is extensive illegal gambling throughout the country. The Indian gambling market is estimated to be worth US$60 billion per year, of which about half is illegally bet. According to the Indian National Newspaper, the chief executive officer for the International Cricket Council (ICC) said he was in favour of legalising betting in sports. He believes the illegal funds profited are through underground bookies that used the money to fund terrorism and drugs. Several Indian institutions have suggested that betting should be regulated and taxed. These include the Committee on Reforms in Cricket in 2015, the Law Commission of India in 2018 and court judgements from the Supreme Court. Many Indian professionals, as well as

online forums, have urged the government to introduce legal but regulated gambling in India to bring the gambling economy out of the grip of mafia and underground dons.
The Public Gambling Act of 1867 - An Act to provide for the punishment of public gambling and the keeping of common gaming houses in India.
The Prize Competition Act of 1955 - The Prize Competition Act was passed by Parliament in 1955 to restrict gambling activities that awarded prizes as winnings. According to the Prize Competition Act, any prize competition where a prize is offered on solving a puzzle, number, alphabet, crossword, missing word, or picture prize competitions, where the winnings more than 1,000 Rupees shall be banned.
The Information Technology Act of 2000 - This law regulates cyber activities in India and does not include any information about gambling or betting". Thus, this document was left for interpretation by the Courts, but they have refused to consider the matter.
In 2022, the Indian government announced its plan on creating a new gaming bill to replace the Public Gambling Act of 1867.
Payment gateways.
One of the biggest obstacles faced by sports bettors in India is the fact that depositing foreign bookies is extremely difficult. Typically, the majority of users deposit to online bookies using Money bookers or Neteller. Some attempts to deposit using a Visa or MasterCard may fail. The same is true of online bank transfers. In order to circumvent these blocks, savvy internet users have started to use e-wallet services for depositing. These services, enable users to fund an online betting account in Rupees. This is important because it avoids legal issues that may have arisen out of F.E.M.A Foreign Exchange law.

An Indian case of Intellectual property crime:

The access, distribution, and/or use of intellectual property without and/or beyond initial authorization and in violation of the rights of the owner or owners of the intellectual property is considered as intellectual property crime (a.k.a., intellectual property theft).

The World Intellectual Property Organization (WIPO) defines *intellectual property* as "creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce." The rights over innovations, creations, original expression of ideas, and secret business practices and processes are protected by national and international intellectual property laws. Under Article 2(viii) of the Convention Establishing the World Intellectual Property Organization of 1967 (amended in 1979), these rights relate to: …literary, artistic and scientific works, …performances of performing artists, phonograms and broadcasts, …inventions in all fields of human endeavor, …scientific discoveries, …industrial designs, …trademarks, service marks and commercial names and designations, …protection against unfair competition, and all other rights resulting from intellectual activity inthe industrial, scientific, literary or artistic fields.
The access, distribution, and/or use of intellectual property without and/or beyond initial authorization and in violation of the rights of the owner or owners of the intellectual property is considered as intellectual property crime (a.k.a., *intellectual property theft*). Because intellectual property rights are recognized as personal property rights (Guan, 2014), intellectual property crime has been considered as a form of theft of personal property, even though it does not match the common understanding of theft (i.e., the deprivation of ownership). For example, if a person's jewellery is stolen, the person is deprived of his/her (tangible) property as the individual no longer has access to the jewellery. In the case of intellectual property, however, even if the property is "stolen" (i.e., used and consumed in an unauthorized way), the holder of the intellectual property *is not* denied his/her property because it is still in the individual's possession. What he/she *is* denied is the control, management, and economic benefit that should be derived from the subsequent use of his/her intellectual property. The deprivation of remuneration for labour (i.e., the creation of intellectual property) serves as a disincentive to the creation of intellectual property, which is

viewed as essential to national economic growth (WIPO, 2009). For this reason, WIPO "promotes innovation and creativity for the economic, social and cultural development of all countries, through a balanced and effective intellectual property system."

Several international conventions, agreements, and treaties (hereafter treaties) have been implemented to protect intellectual property rights. A case in point is the Berne Convention for the Protection of Literary and Artistic Works of 1886(as amended in 1979), which delineates the obligation of states to protect intellectual property and the minimum standards for intellectual property protection. Due to concerns about the enforcement of the Berne Convention, the World Trade Organization's (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) of 1994 (which entered into force in 1995) was passed. The TRIPS Agreement requires WTO countries to fulfil their obligations under the Berne Convention, among other treaties. The World Trade Organization oversees the administration of the TRIPS agreement, and provides, among other things, standards for intellectual property policies, laws and regulations, and enforcement mechanisms for the protection of intellectual property rights.

Financial Frauds in Cyber Domain:

Most critical functions of twenty-first-century society have become inextricably dependent on digital infrastructure, in particular the financial industry, whose business model relies on consumer confidence in the overall financial system. The internet is now the primary mechanism for financial transfers between banks and other institutions; most customers rely on online banking to manage their accounts and for the majority of point of sale payments. In fact, Canada ranks among the most cashless societies in the world (ForexBonuses 2017). The more reliant on digital technology the financial system becomes, the more interconnected it is and the more vulnerable it is to cyber exploitation. Consumers notoriously prefer convenience over security, and financial institutions encourage consumers to use online technology as a way of harnessing efficiencies and reducing operating costs. Malicious actors are not targeting the industry for mere financial gain: because the financial industry is systemically significant, adversaries are actively looking to exploit vulnerabilities that could be used to bring it down, thereby undermining confidence in the financial system and causing social chaos and turmoil to threaten the democratic way of life. The financial industry’s dense interconnectivities, broad digital footprint with consumers and extensive reliance on technological infrastructure expose it to a disproportionately large attack surface. Governance at both the national and the international level has not kept up.