INSTITUTEOFAERONAUTICALENGINEERING

(AUTONOMOUS)

Dundigal,Hyderabad-500043

LECTURE NOTES:

FOUNDATIONS OF CYBER SECURITY

DRAFTED BY :

ALEKHYA JUTTIGA(IARE10872)
AssistantProfessor

DEPARTMENT OF CYBER SECURITY

INSTITUTE OF AERONAUTICAL ENGINEERING

Nov 25,2021

Contents

4 CYBER SECURITY: ORGANIZATIONAL IMPLICATIONS

5 CYBERCRIME: EXAMPLES AND MINI-CASES EXAMPLES

List of Figures:

Abbreviations:

GDPA: General Data Protection Act
CIA: Confidentiality, Integrity and Availability
NIC: National Informatics Center
VSAT: Very Small Aperture Terminal
ISP: Internet Service Providers
ERNT: Education and Research Network
NSA: National Security Agency
PDP: Policy Development Process
GTD: GPRS Tunneling Protocol
GPRS: General Packet Radio Service
IMS: IP Multimedia Subsystem
SIP: Session Initiation Protocol

Chapter 1

INTRODUCTION TO CYBER SECURITY

Course Outcomes

After successful completion of this module, students should be able to:

CO1	Explain Basic Cyber Security Concepts to overcome thecyber-attacks	Understand

1.1 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-scalebusinessesorlargeorganization,areallbeingimpacted.So,allthesefirmswhether ITornon-ITfirmshaveunderstoodtheimportanceofCyberSecurityandfocusingonadopting all possible measures to deal with cyberthreats.

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 informationsystem.

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 informationsecurity.

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 toendure.
- In addition to financial damage suffered by the business, a data breach can also inflict untold reputationaldamage.
- 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 theyhold.

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 whenhe has a good grip on cyber securityfundamentals.

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:

- Dataencryption
- Two-factorauthentication
- Biometricverification
- Securitytokens

Integrity:

Integrity refers to protecting information from being modified by unauthorized parties.
Standard measures to guarantee integrity include:

- Cryptographicchecksums
- Using filepermissions
- Uninterrupted powersupplies
- Databackups

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 externaldrives
- Implementingfirewalls
- Having backup powersupplies
- Dataredundancy

1.2 Layers of cyber security:

The 7 layers of cyber security should center 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'saccesstoyourmissioncriticalassets,andtheinternalsecurityoftheapplication.
4. Endpoint Security – Endpoint security controls protect the connection between devices and thenetwork.
5. NetworkSecurity–Networksecuritycontrolsprotectanorganization'snetworkandprevent unauthorized access of thenetwork.
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.

1.3 Vulnerability, threat, Harmful acts

As the recent epidemic of data breaches illustrates, no system is immune to attacks. Any companythatmanages,transmits,stores,orotherwisehandlesdatahastoinstituteand enforce mechanismstomonitortheircyberenvironment,identifyvulnerabilities,andcloseupsecurity holes as quickly aspossible.

Before identifying specific dangers to modern data systems, it is crucial to understand the distinction between cyber threats and vulnerabilities.

1.4 Cyber threats

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.

1.5 Vulnerabilities

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 ofavailability)

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

Attacks are threats that have been carriedout.

- Passive–Makeuseofinformationfromthesystemwithoutaffectingsystemresources
- Active – Alter system resources or affectoperation
- Insider – Initiated by an entity inside theorganization
- Outsider – Initiated from outside theperimeter

1.6 Internet Governance – Challenges and Constraints:

Most organizations have good enterprise-level security policies that define their approach to maintaining, improving, and securing their information and information systems. However, once the policies are signed by senior leadership and distributed throughout the organization, significant cybersecurity governance challenges remain. Let us discuss five fundamental challenges of cybersecurity governance that are essential to establishing and maintaining an effective cybersecurity governance program.

The ISO/IEC 27001 standard, from the International Organization for Standardization (ISO) and International Electro technical Commission (IEC), defines IT governance as, "The system by which an organization directs and controls security governance, specifies the accountability framework and provides oversight to ensure that risks are adequately mitigated, while management ensures that controls are implemented to mitigate risks."

In an increasingly challenging threat landscape, many organizations struggle with implementing and enforcing effective cybersecurity governance. The CERT Division's research in this field derives from conducting various organizational assessments, including Cyber Resilience Reviews (CRRs), External Dependencies Management (EDM) Assessments, and Information Security Continuous Monitoring Assessments (ISCMs). The CRR and EDM assessments derive from the CERT Resilience Management Model (CERT-RMM), a maturity model for managing operational resilience and a leading resource for process improvement.

Many organizations we have assessed seem to struggle with five fundamental challenges to cybersecurity governance:

1. Cybersecurity Strategy and Goals
2. Standardized Processes
3. Enforcement and Accountability
4. Senior Leadership Oversight
5. Resources

1. Cybersecurity Strategy and Goals:

To establish a good cybersecurity governance program, the organization must clearly define its risk management policies, strategy, and goals. Senior leadership must assess their current risk management approach prior to defining the strategy and goals for the organization's preferred state. The strategy should be a high-level document that establishes the roadmap for the organization to maintain and improve its overall risk management approach. Once the strategy and goals are finalized, an enterprise-level policy must be implemented and distributed throughout the organization

Key components to developing an effective cybersecurity strategy include

- understanding how cybersecurity risk relates to your critical business operations
- developing strategic goals for the organization
- defining the scope
- identifying cybersecurity needs and develop objectives
- establishing key performance indicators (KPIs)
- determining resource needs
- determining risk appetite
- establishing continuous monitoring

2. Standardized Processes:

Many organizations have processes and personnel to ensure that daily tasks are completed. However, management of specific tasks--if they're managed at all--isn't always done as effectively as it could be. Without approved, standardized processes that are repeatable, organizations cannot ensure efficiency, quality, or **consistency**. Consistency is critical to ensure a common understanding and management approach to risks throughout the organization. Establishing repeatable processes is a key factor to an organization's overall cybersecurity governance program. In short, a cybersecurity governance program that is ad-hoc and inconsistent will eventually lead to shortfalls. An ineffective cybersecurity governance program will lead to increased security breaches, compromises, and attacks.

3. Enforcement and Accountability:

Processes should be in place to enforce requirements. Otherwise, the cybersecurity program will become inconsistent, requirements will be ignored, and failure will occur. Once those with program responsibilities perceive or observe that accountability and cybersecurity governance are lacking, they will come up with their own way of doing things, which is counter to establishing standardized processes. Cybersecurity governance must be measurable and enforced, and there must be accountability for compliance across all personnel levels.

The National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) recommends a tiered approach to risk management and promotes the development of security and privacy capabilities into information systems throughout the system development life cycle (SDLC). This approach can be accomplished by continuously monitoring those systems to maintain situational awareness of their security and privacy posture. Information should also be provided to senior leaders and executives to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, and other organizations. Part 2 of this series, Addressing Cybersecurity Governance Challenges, will look more deeply into the NIST tiered approach to risk management.

4. Senior Leadership Oversight:

Because cybersecurity governance is an enterprise concern, the focus and direction for the cybersecurity program must come from the top to ensure that the process is achieving its goals. Unless senior leadership supports cybersecurity governance with a strong "tone at the top" approach, the organization's risk management efforts will most likely fail. Senior leadership must remain engaged for the lifecycle of the program. This engagement helps to ensure that the entire organization not only understands senior leadership's commitment to cybersecurity governance, but is implementing it at a high standard. ISO 27001, section five, has a list of leadership principles that are relevant in establishing an effective cybersecurity governance program:

- ensuring the information security policy and the information security objectives are established, and are compatible with the strategic direction of the organization
- ensuring information security management system requirements are integrated into the organization's processes
- ensuring that the resources needed for the information security management system are available
- communicating the importance of effective information security management, and conforming to the information security management system requirements
- ensuring that the information security management system achieves its intended outcomes
- directing and supporting staff to contribute to the effectiveness of the information security management system
- promoting continual improvements

Top management shall establish a cybersecurity policy that:

- is appropriate to the purpose of the organization
- includes information security objectives or the framework for setting information security objectives
- includes a commitment to satisfy applicable requirements related to information security
- includes a commitment to continual improvement of the information security management system
- is available as documented information
- is communicated within the organization and is available to relevant parties, as appropriate

5. Resources:

Senior leadership must ensure adequate resources are available to meet basic cybersecurity governance and compliance needs commensurate with the organization's cybersecurity strategy and goals. Funding must be allocated to the highest priorities to secure information and information systems, adequate for the levels of risk. Resourcing must also include dedicated funding for qualified personnel and their training. In addition, resources must allow for the procurement of sufficient tools for adequately measuring KPIs as well as maintaining repeatable processes.

1.7 Computer Criminals:

Computer criminals have access to enormous amounts of hardware, software, and data; they havethepotentialtocripplemuchofeffectivebusinessandgovernmentthroughouttheworld. In a sense, the purpose of computer security is to prevent these criminals from doingdamage.

We say computer crimeis any crime involving a computer or aided by the use of one. Althoughthisdefinitionisadmittedlybroad,itallowsustoconsiderwaystoprotectourselves, our businesses, and our communities against those who use computersmaliciously.

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.

Common Types of Cyber Criminals:

Cyber criminals, also known as hackers, often use computer systems to gain access to business trade secrets and personal information for malicious and exploitive purposes. Hackers are extremely difficult to identify on both an individual and group level due to their various security measures, such as proxies and anonymity networks, which distort and protect their identity. Cybersecurity experts assert that cyber criminals are using more ruthless methods to achieve their objectives and the proficiency of attacks is expected to advance as they continue to develop new methods for cyber attacks. The growth of the global cyber criminal network, which is largely credited to the increased opportunity for financial incentives, has created a number of different types of cyber criminals, many of which pose a major threat to governments and corporations.

1. Identity Thieves:

Identity thieves are cyber criminals who try to gain access to their victims' personal information – name, address, phone number, place of employment, bank account, credit card information and social security number. They use this information to make financial transactions while impersonating their victims. Identity theft is one of the oldest cyber-crimes, gaining prominence during the early years of the Internet. Initially, these cyber criminals leveraged basic hacking techniques, such as modifying data and leveraging basic identity fraud to uncover the desired information. Today, the practice has progressed in scope and technique due to advances in computing, and now, many identity thieves can hack into a government or corporate database to steal a high-volume of identities and personal information. This expansion of strategy has resulted in major losses for companies and consumers, with recent studies indicating that approximately $112 billion has been stolen by identity thieves over the past six years.

2. Internet Stalkers:

Internet stalkers are individuals who maliciously monitor the online activity of their victims to terrorize and/or acquire personal information. This form of cyber crime is conducted through the use of social networking platforms and malware, which are able to track an individual's computer activity with very little detection. The motives for such attacks can differ depending on the cyber criminal, but many internet stalkers seek to acquire important information that they can use for bribery, slander, or both. Businesses should be aware of internet stalkers, as well as the strategies that they utilize, in case their employees are ever victims of this cyber attack. If left unaddressed, internet stalkers could cause emotional distress to the team or even obtain data for blackmail.

3. Phishing Scammers:

Phishers are cyber criminals who attempt to get ahold of personal or sensitive information through victims' computers. This is often done via phishing websites that are designed to copycat small-business, corporate or government websites. Unsuspecting computer users often fall prey to such activities by unknowingly providing personal information including home addresses, social security numbers, and even bank passwords. Once such information is obtained, phishers either use the information themselves for identity fraud scams or sell it in the dark web. It's important for businesses to constantly be aware of phishing scams, particularly scams that may be trying to copycat their own business site. Such sites can tarnish the company's reputation and brand, which could potentially lead to a decrease in earnings.

4. Cyber Terrorists:

Cyber terrorism is a well-developed, politically inspired cyber attack in which the cyber criminal attempts to steal data and/or corrupt corporate or government computer systems and networks, resulting in harm to countries, businesses, organizations, and even individuals. The key difference between an act of cyberterrorism and a regular cyber attack is that within an act of cyber terrorism, hackers are politically motivated, as opposed to just seeking financial gain.

1.8 CIA Triad:

The CIA Triad is actually a security model that has been developed to help people thinkabout various parts of ITsecurity.

CIA triad broken down:

Confidentiality:

It's crucial in today's world for people to protect their sensitive, private information from unauthorized access. Protectingconfidentialityisdependentonbeingabletodefineandenforcecertainaccesslevels forinformation.

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.

Standard measures to establish confidentiality include:

- Dataencryption
- Two-factorauthentication
- Biometricverification
- Securitytokens

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 modificationfromanyunauthorizedparty,anditensuresthatwhenanauthorizedpersonmakes a change that should not have been made the damage can bereversed.

Standard measures to guarantee integrity include:

- Cryptographicchecksums
- Using filepermissions
- Uninterrupted powersupplies
- Databackups

Availability

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

Standard measures to guarantee availability include:

- Backing up data to externaldrives
- Implementingfirewalls
- Having backup powersupplies
- Dataredundancy

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 resourcesneededtoprovideinformationwhenitisneeded,thinkingaboutinformationsecurity in itself doesn't guarantee that someone else hasn't used your hardware resources without authorization.

It'simportanttounderstandwhattheCIATriadis,howitisusedtoplanandalsotoimplement aqualitysecuritypolicywhileunderstandingthevariousprinciplesbehindit.It'salsoimportant tounderstandthelimitationsitpresents.Whenyouareinformed,youcanutilizetheCIATriad for what it has to offer and avoid the consequences that may come along by notunderstanding it.

1.9 Assets and Threat:

WhatisanAsset:Anassetisanydata,deviceorothercomponentofanorganization'ssystems that is valuable – often because it contains sensitive data or can be used to access such information.

Forexample:Anemployee'sdesktopcomputer,laptoporcompanyphonewouldbeconsidered an asset, as would applications on those devices. Likewise, critical infrastructure, such as serversandsupportsystems,areassets.Anorganization'smostcommonassetsareinformation 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.

1.10 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 availabilityofthecorrectpersontotakeactionOfprimaryconcernherearedeliberateactions, of which there are three categories ofmotivation.

1. **Political motivations**: examples include destroying, disrupting, or taking control of targets; espionage; and making political statements, protests, or retaliatoryactions.
2. **Economic motivations**: examples include theft of intellectual property or other economically valuable assets (e.g., funds, credit card information); fraud;industrial espionage and sabotage; andblackmail.
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.

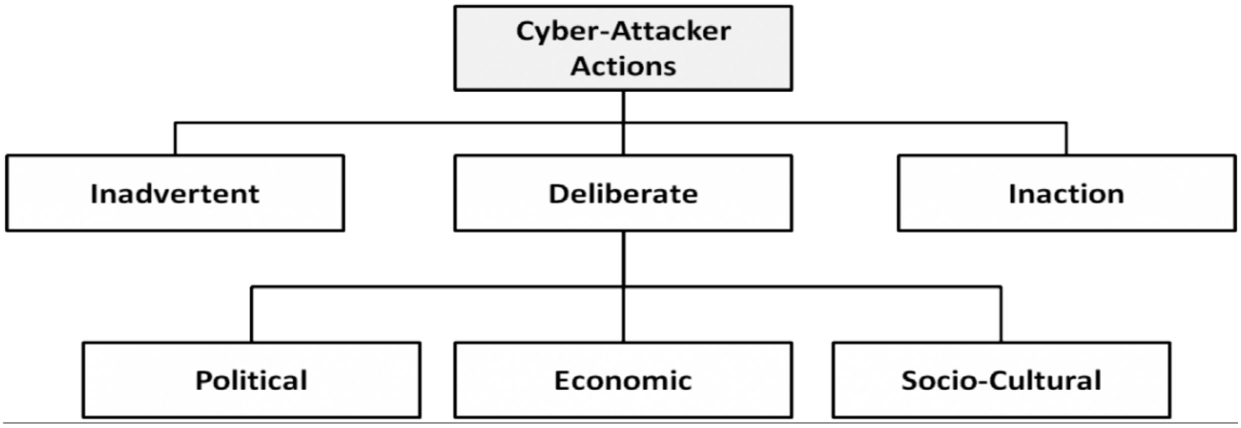


Fig 1.1: Types of cyber-attacker actions and their motivations when deliberate

1.11 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.

Ina**denialofservice(DoS)**attack,users aredeprivedofaccesstoanetworkorwebresource. Thisisgenerallyaccomplishedbyoverwhelmingthetargetwithmoretrafficthanitcanhandle.

In a **distributed denial-of-service** **(DDoS)** exploit, large numbers of compromised systems (sometimes called a botnet or zombie army) attack a single target.

PassiveAttacks:

Passiveattacksarerelativelyscarcefromaclassificationperspective,butcan be carried out with relative ease, particularly if the traffic is notencrypted.

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 analysiscanalsoleadtoattacksbycryptanalysis,wherebytheattackermayobtaininformation or succeed in unencrypting thetraffic.

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 very difficult to remove and very damaging.

Common malware examples are listed in the following table:

Attack	Characteristics
Virus	A virus is a program that attempts to damage a computer system and replicate itself to other computer systems. A virus: • Requires a host to replicate and usually attaches itself to a host file ora hard drivesector. • Replicates each time the host isused. • Often focuses on destruction or corruption ofdata. • Usually attaches to files with execution capabilities such as .doc,.exe, and .batextensions. • Often distributes via e-mail. Many viruses can e-mail themselvesto everyone in your addressbook. • Examples: Stoned, Michelangelo, Melissa, I LoveYou.
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 of replicating itself. A worm: • Can install a backdoor in the infectedcomputer. • Is usually introduced into the system through avulnerability. • Infects one system and spreads to other systems on thenetwork. • Example: CodeRed.
Trojan horse	A Trojan horse is a malicious program that is disguised as legitimate software. Discretionary environments are often more vulnerable and susceptible to Trojan horse attacks because security is user focused and user directed. Thus the compromise of a user account could lead to the compromise of the entire environment. A Trojan horse: • Cannot replicateitself. • Often contains spying functions (such as a packet sniffer) orbackdoor functions that allow a computer to be remotely controlled from the network. • Often is hidden in useful software such as screen savers orgames. • Example: Back Orifice, Net Bus,Whack-a-Mole.
Logic Bomb	A Logic Bomb is malware that lies dormant until triggered. A logic bomb is a specific example of an asynchronous attack. • A trigger activity may be a specific date and time, the launching ofa specific program, or the processing of a specific type ofactivity. • Logic bombs do notself-replicate.

1.12 Cyber Threats-Cyber Warfare, Cyber Crime, Cyber terrorism, Cyber Espionage:

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 network oranetworkeddevice.Cybercrimeiscommittedbycybercriminalsorhackerswhowantto make money. Cybercrime is carried out by individuals ororganizations.

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.

Cyber Espionage:

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

1.13 Comprehensive Cyber Security Policy:

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

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

We use security policies to manage our network security. Most types of security policies are automaticallycreatedduringtheinstallation.Wecanalsocustomizepoliciestosuitourspecific environment.

Need of Security policies-

1) It increasesefficiency.
2) It upholds discipline and accountability
3) It can make or break a businessdeal
4) It helps to educate employees on securityliteracy

There are some important cyber security policies recommendations describe below.

Virus and Spyware Protection policy:

- Ithelpstodetectthreadsinfiles,todetectapplicationsthatexhibitsuspiciousbehavior.
- Removes, and repairs the side effects of viruses and security risks by usingsignatures.

Firewall Policy:

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

Intrusion Prevention policy:

- This policy automatically detects and blocks the network attacks and browserattacks.
- Italsoprotectsapplicationsfromvulnerabilitiesandchecksthecontentsofoneormore data packages and detects malware which is coming through legalways.

Application and Device Control:

- Thispolicyprotects asystem'sresourcesfromapplicationsandmanagestheperipheral devices that can attach to asystem.
- The device control policy applies to both Windows and Mac computers whereas application control policy can be applied only to Windowsclients.

Chapter 2

CYBER SPACE AND THE LAW & CYBER FORENSICS

Course Outcomes

After successful completion of this module, students should be able to:

CO2	Select cyberspace and the law to offer reliable legal inclusiveness to facilitating registration of real-time records.	Apply
CO3	Relate forensic investigation and challenges in computer forensics to gather and preserve evidence.	Understand

2.1 Introduction:

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.

Withthebenefitscarriedbythetechnologicaladvancements,thecyberspacetodayhasbecome 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 toit.

2.2 Cyber Security Regulations

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

Information Technology Act, 2000 The Indian cyber laws are governed by the Information Technology Act, penned down back in 2000. The principal impetus of this Act is to offer reliable legal inclusiveness to eCommerce, facilitating registration of real-time records with the Government. But with the cyber attackers getting sneakier, topped by the human tendency to misuse technology, a series of amendments followed.

TheITA,enactedbytheParliamentofIndia,highlightsthegrievouspunishmentsandpenalties safeguarding the e-governance, e-banking, and e-commerce sectors. Now, the scope of ITA has been enhanced to encompass all the latest communicationdevices. The IT Act is the salient one, guiding the entire Indian legislation to govern cybercrimes rigorously:

Section43-Applicabletopeoplewhodamagethecomputersystemswithoutpermissionfrom the owner. The owner can fully claim compensation for the entire damage in suchcases.

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 devicesorcomputers,whichconfirmsaprobablethreeyearsimprisonment.Thistermcanalso be topped by Rs. 1 lakh fine, depending upon theseverity.

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

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

Indian Penal Code (IPC) 1980

Identity thefts and associated cyber frauds are embodied in the Indian Penal Code (IPC), 1860 invoked along with the Information Technology Act of 2000. The primary relevant section of the IPC covers cyberfrauds:

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

ThecorporatestakeholdersrefertotheCompaniesActof2013asthelegalobligationnecessary 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 legalfix.

TheCompaniesAct2013vestedpowersinthehandsoftheSFIO(SeriousFraudsInvestigation 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 thisregard.

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

NIST Compliance

The Cybersecurity Framework (NCFS), authorized by the National Institute of Standards and Technology(NIST),offersaharmonizedapproachtocybersecurityasthemostreliableglobal certifyingbody.

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

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

FinalThoughtsAshumandependenceontechnologyintensifies,cyberlawsinIndiaandacross the globe need constant up-gradation and refinements. The pandemic has also pushed muchof the workforce into a remote working module increasing the need for app security. Lawmakers havetogotheextramiletostayaheadoftheimpostors,inordertoblockthemattheiradvent.

Cybercrimes can be controlled but it needs collaborative efforts of the lawmakers, theInternet or Network providers, the intercessors like banks and shopping sites, and, most importantly, theusers.Onlytheprudenteffortsofthesestakeholders,ensuringtheirconfinementtothelaw of the cyber land can bring about online safety andresilience.

2.3 ROLES OF INTERNATIONAL LAW:

In various countries, areas of the computing and communication industries are regulated by governmental bodies. There are specific rules on the uses to which computers and computer networks may be put, in particular there are rules on unauthorized access, data privacy and spamming. There are also limits on the use of encryption and of equipment which may be used to defeat copy protection schemes

- There are laws governing trade on the Internet, taxation, consumer protection, and advertising
- There are laws on censorship versusfreedom of expression, rules on public access to government information, and individual access to information held on them by private bodies Some states limit access to the Internet, by law as well as by technicalmeans.

INTERNATIONAL LAW FOR CYBER CRIME

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

2.4 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(theNICNW)anationwideverysmallapertureterminal(VSAT)NW for public sector organizations as well as to connect the central govt with the state govts and district administrations, the third NW setup was ERNET (the Education and Research Network), to serve the academic and researchcommunities.

New Internet Policy of 1998 paved the way for services from multiple Internet service providers(ISPs)andgaveboosttotheInternetuserbasegrowfrom1.4millionin1999toover 150 million by Dec 2012. Exponential growth rate is attributed to increasing Internet access throughmobilephonesandtablets.Govtismakingadeterminedpushtoincreasebroadbandpenetration from its present level of about 6%1. The target for broadband is 160 million households by 2016 under the National Broadband Plan

2.5 NATIONAL CYBER SECURITY POLICY:

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

VISION:

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

MISSION:

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

OBJECTIVE:

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

- To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of theeconomy.
- Tocreateanassuranceframeworkforthedesignofsecuritypoliciesandpromotionand 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 recoveryactions.

2.6 INTRODUCTION TO 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 anythingfrombreakingencryption,toexecutingsearchwarrantswithalawenforcement team, to recovering and analyzing files from hard drives that will be critical evidence in the most serious civil and criminalcases.

The forensic examination of computers, and data storage media, is a complicated and highly specializedprocess.Theresultsofforensicexaminationsarecompiledandincludedinreports. In many cases, examiners testify to their findings, where their skills and abilities are put to ultimatescrutiny.

2.7 HISTORICAL BACKGROUND OF CYBER FORENSICS:

It is difficult to pinpoint when computer forensics history began. Most experts agree that the field of computer forensics began to evolve more than 30 years ago. The field began in the United States, in large part, when law enforcement and military investigators started seeing criminals get technical. Government personnel charged with protecting important, confidential, and certainly secret information conducted forensic examinations in response to potential security breaches to not only investigate the particular breach, but to learn how to prevent future potential breaches. Ultimately, the fields of information security, which focuses on protecting information and assets, and computer forensics, which focuses on the response to hi-tech offenses, started to intertwine.

Over the next decades, and up to today, the field has exploded. Law enforcement and the military continue to have a large presence in the information security and computer forensic field at the local, state, and federal level. Private organizations and corporations have followed suit – employing internal information security and computer forensic professionals or contracting such professionals or firms on an as-needed basis. Significantly, the private legal industry has more recently seen the need for computer forensic examinations in civil legal disputes, causing an explosion in the e-discovery field.

The computer forensic field continues to grow on a daily basis. More and more large forensic firms, boutique firms, and private investigators are gaining knowledge and experience in the field. Software companies continue to produce newer and more robust forensic software programs. And law enforcement and the military continue to identify and train more and more of their personnel in the response to crimes involving technology.

2.8 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.

2.9THE NEED FOR COMPUTER FORENSICS:

Computer forensics is also important because it can save your organization money. Froma
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.

2.10 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 evidenceiscommonlyassociatedwithelectroniccrime,ore-crime,suchaschildpornography 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 10victims.

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.

2.11 FORENSICS ANALYSIS OF EMAIL:

E-mail forensics refers to the study of source and content of e-mail as evidence to identify the actual sender and recipient of a message, data/time of transmission, detailed record of e-mail transaction, intent of the sender, etc. This study involves investigation of metadata, keyword searching, port scanning, etc. for authorship attribution and identification of e-mail scams.

Various approaches that are used for e-mail forensic are:

HeaderAnalysis–Metadatainthee-mailmessageintheformofcontrolinformation i.e. envelope and headers including headers in the message body contain information aboutthesenderand/orthepathalongwhichthemessagehastraversed.Someofthese may be spoofed to conceal the identity of the sender. A detailed analysis of these headers and their correlation is performed in headeranalysis.

Bait Tactics – In bait tactic investigation an e-mail with http: "<imgsrc>" tag having image source at some computer monitored by the investigators is send to the sender of e-mailunderinvestigationcontainingreal(genuine)e-mailaddress.Whenthee-mailis opened,alogentrycontainingtheIPaddressoftherecipient(senderofthee-mailunder investigation) is recorded on the http server hosting the image and thus sender is tracked. However, if the recipient (sender of the e-mail under investigation) is using a proxy server then IP address of the proxy server is recorded. The log on proxy server can be used to track the sender of the e-mail under investigation. If the proxy server's log is unavailable due to some reason, then investigators may send the tactic e-mail containinga)EmbeddedJavaAppletthatrunsonreceiver'scomputerorb)HTMLpage withActiveXObject.BothaimingtoextractIPaddressofthereceiver'scomputerand e-mail it to theinvestigators.

ServerInvestigation–Inthisinvestigation,copiesofdeliverede-mailsandserverlogs are investigated to identify source of an e-mail message. E-mails purged from the clients (senders or receivers) whose recovery is impossible may be requested from servers (Proxy or ISP) as most of them store a copy of all e-mails after theirdeliveries. Further, logs maintained by servers can be studied to trace the address of the computer responsible for making the e-mail transaction. However, servers store the copies of e- mail and server logs only for some limited periods and some may not co-operate with the investigators. Further, SMTP servers which store data like credit card number and otherdatapertainingtoownerofamailboxcanbeusedtoidentifypersonbehindane- mailaddress.

Network Device Investigation – In this form of e-mail investigation, logs maintained by the network devices such as routers, firewalls and switches are used to investigate thesourceofane-mailmessage.Thisformofinvestigationiscomplexandisusedonly when the logs of servers (Proxy or ISP) are unavailable due to some reason, e.g. when ISP or proxy does not maintain a log or lack of co-operation by ISP's or failure to maintain chain ofevidence.

Software Embedded Identifiers – Some information about the creator of e-mail, attachedfilesordocumentsmaybeincludedwiththemessagebythee-mailsoftwareusedbythesenderforcomposinge-mail.Thisinformationmaybeincludedintheform ofcustomheadersorintheformofMIMEcontentasaTransportNeutralEncapsulation Format (TNEF). Investigating the e-mail for these details may reveal some vital informationaboutthesenderse-mailpreferencesandoptionsthatcouldhelpclientside evidence gathering. The investigation can reveal PST file names, Windows logon username, MAC address, etc. of the client computer used to send e-mailmessage.

SenderMailerFingerprints–Identificationofsoftwarehandlinge-mailatservercan be revealed from the Received header field and identification of software handling e- mail at client can be ascertained by using different set of headers like "X-Mailer" or equivalent.Theseheadersdescribeapplicationsandtheirversionsusedattheclientsto send e-mail. This information about the client computer of the sender can be used to help investigators devise an effective plan and thus prove to be veryuseful.

EMAIL FORENSICS TOOLS

Erasing or deleting an email doesn't necessarily mean that it is gone forever. Often emailscan be forensically extracted even after deletion. Forensic tracing of e-mail is similar totraditional detective work. It is used for retrieving information from mailboxfiles.

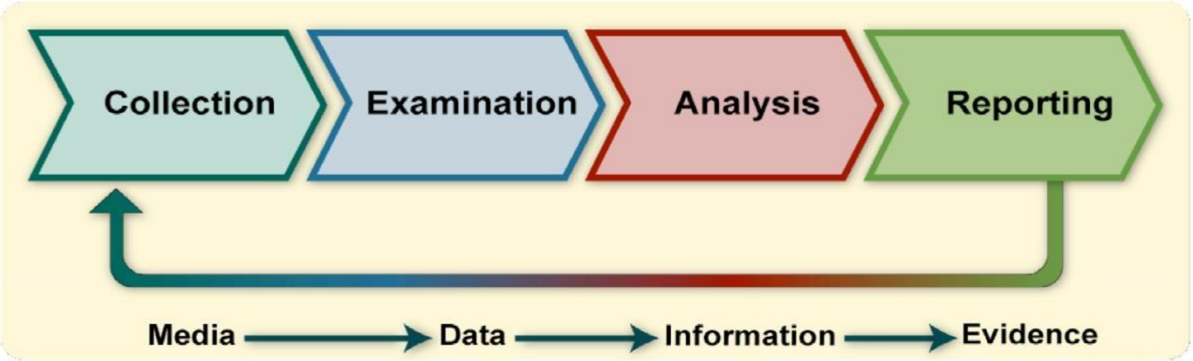
MiTec Mail Viewer – This is a viewer for Outlook Express, Windows Mail/Windows LiveMail,MozillaThunderbirdmessagedatabases,andsingleEMLfiles.Itdisplaysa list of contained messages with all needed properties, like an ordinary e-mail client. Messages can be viewed in detailed view, including attachments and an HTML preview. It has powerful searching and filtering capability and also allows extracting emailaddressesfromallemailsinopenedfoldertolistbyoneclick.Selectedmessages can be saved to eml files with or without their attachments. Attachments can be extracted from selected messages by one command.

OST and PST Viewer – Nucleus Technologies' OST and PST viewer tools help you view OST and

PST files easily without connecting to an MS Exchange server. These tools allow the user to scan OST and PST files and they display the data saved in it including email messages, contacts, calendars, notes, etc., in a proper folderstructure.

eMailTrackerPro– eMailTrackerPro analyses the headers of an e-mail to detect the IPaddressofthemachinethatsentthemessagesothatthesendercanbetrackeddown. It can trace multiple e-mails at the same time and easily keep track of them. The geographical location of an IP address is key information for determining the threat level or validity of an e-mailmessage.

EmailTracer– EmailTracer is an Indian effort in cyber forensics by the Resource Centre for Cyber Forensics (RCCF) which is a premier centre for cyber forensics in India. It develops cyber forensic tools based on the requirements of law enforcement agencies.



2.12 DIGITAL FORENSICS LIFECYCLE:

There are many type of Cyber crimes taking place in the digital world, it is important for the investigator to collect, analyze, store and present the evidence in such a manner that court will believe in such digital evidences and give appropriate punishment to the Cyber criminal.

Fig 2.1: Digital Forensics Lifecycle

Collection: The first step in the forensic process is to identify potential sources of data and acquire data from them.

Examination: After data has been collected, the next phase is to examine the data, which involves assessing and extracting the relevant pieces of information from the collected data. This phase may also involve bypassing or mitigating OS or application features that obscure data and code, such as data compression, encryption, and access control mechanisms.

Analysis: Once the relevant information has been extracted, the analyst should study and analyzethedatatodrawconclusionsfromit.Thefoundationofforensicsisusingamethodical approach to reach appropriate conclusions based on the available data or determine that no conclusion can yet bedrawn.

Reporting: Theprocessofpreparingandpresentingtheinformationresultingfromtheanalysis phase. Many factors affect reporting, including thefollowing:

a.**Alternative Explanations:**When the information regarding an event is incomplete, it may not be possible to arrive at a definitive explanation of what happened. When an event has two or more plausible explanations, each should be given due consideration inthereportingprocess.Analystsshoulduseamethodicalapproachtoattempttoprove or disprove each possible explanation that isproposed.

b. **AudienceConsideration.**Knowingtheaudiencetowhichthedataorinformationwill be shown isimportant.

c.**Actionable Information.** Reporting also includes identifying actionable information gained from data that may allow an analyst to collect new sources ofinformation.

2.13 FORENSICS INVESTIGATION:

Forensics are the scientific methods used to solve a crime. Forensic investigation is the gathering and analysis of all crime-related physical evidence in order to come to a conclusion about a suspect. Investigators will look at blood, fluid, or fingerprints, residue, hard drives, computers,orothertechnologytoestablishhowacrimetookplace.Thisisageneraldefinition, though, since there are a number of different types offorensics.

TYPES OF FORENSICS INVESTIGATION

- Forensic Accounting /Auditing
- Computer or CyberForensics
- Crime SceneForensics
- ForensicArchaeology
- ForensicDentistry
- ForensicEntomology
- ForensicGraphology
- ForensicPathology
- ForensicPsychology
- ForensicScience
- ForensicToxicology

2.14CHALLENGES IN COMPUTER FORENSICS:

Digital forensics has been defined as the use of scientifically derived and proven methods towards the identification, collection, preservation, validation, analysis, interpretation, and presentation of digital evidence derivative from digital sources to facilitate the reconstruction of events found to be criminal.But these digital forensics investigation methods face some major challenges at the time of practical implementation. Digital forensic challenges are categorized into three major heads as per Fahdi, Clark, and Furnell are:

- Technicalchallenges
- Legalchallenges
- ResourceChallenges

TECHNICAL CHALLENGES

As technology develops crimes and criminals are also developed with it. Digital forensic expertsuseforensictoolsforcollectingshredsofevidenceagainstcriminalsandcriminalsuse such tools for hiding, altering or removing the traces of their crime, in digital forensic this process is called Anti- forensics technique which is considered as a major challenge in digital forensics world.

Anti-forensics techniques are categorized into the following types:

S. No.	Type	Description
1	Encryption	It is legitimately used for ensuring the privacy of information by keeping it hidden from an unauthorized user/person. Unfortunately, it can also be used by criminals to hide their crimes
2	Data hiding in storage space	Criminals usually hide chunks of data inside the storage medium in invisible form by using system commands, and programs.

3	Covert Channel	Acovertchannelisacommunicationprotocolwhich allows an attacker to bypass intrusion detection technique and hide data over the network. The attackeruseditforhidingtheconnectionbetween him and the compromised system.

Other Technical challenges are:

- Operating in thecloud
- Time to archive data
- Skillgap
- Steganography

LEGAL CHALLENGES

Thepresentationofdigitalevidenceismoredifficultthanitscollectionbecausetherearemany instances where the legal framework acquires a soft approach and does not recognize every aspectofcyberforensics,as inJagdeoSinghV.TheStateandOrscaseHon'bleHighCourtof Delhi held that "while dealing with the admissibility of an intercepted telephone call in a CD and CDR which was without a certificate under Sec. 65B of the Indian Evidence Act, 1872the court observed that the secondary electronic evidence without certificate u/s. 65B of Indian Evidence Act, 1872 is not admissible and cannot be looked into by the court for any purpose whatsoever." This happens in most of the cases as the cyber police lack the necessary qualification and ability to identify a possible source of evidence and prove it. Besides, most of the time electronic evidence is challenged in the court due to its integrity. In the absence of properguidelinesandthenonexistenceofproperexplanationofthecollection,andacquisition of electronic evidence gets dismissed initself.

Legal Challenges:

S.No.	Type	Description
1	Absence of guidelines and standards	In India, there are no proper guidelines for the collection and acquisition of digital evidence. The investigating agencies and forensic laboratories are working on the guidelines of their own. Due to this, the potential of digital evidence has been destroyed.
2	Limitation of the Indian Evidence Act,1872	TheIndianEvidenceAct,1872havelimitedapproach, it is not able to evolve with the time and address the E-evidence are more susceptible to tampering, alteration, transposition, etc. the Act is silent on the method of collection of e-evidence it only focuses on the presentation of electronic evidence in the court by accompanying a certificate as per subsection 4 ofSec. 65B[12]. This means no matter what procedure is followeditmustbeprovedwiththehelpofa certificate.

Other Legal Challenges

- PrivacyIssues
- Admissibility inCourts
- Preservation of electronicevidence
- Power for gathering digitalevidence
- Analyzing a runningcomputer

RESOURSE CHALLENGES:

Astherateofcrimeincreasesthenumberofdataincreasesandtheburdentoanalyzesuchhuge dataisalsoincreasingonadigitalforensicexpertbecausedigitalevidenceismoresensitiveas compared to physical evidence it can easily disappear. For making the investigation process fast and useful forensic experts use various tools to check the authenticity of the data but dealing with these tools is also a challenge initself.

Types of Resource Challenges are:

Change intechnology:

Due to rapid change in technology like operating systems, application software and hardware, reading of digital evidence becoming more difficult because new version software's are not supportedtoanolderversionandthesoftwaredevelopingcompaniesdidprovideanybackward compatible's which also affectslegally.

Volume andreplication:

The confidentiality, availability, and integrity of electronic documents are easily get manipulated. The combination of wide-area networks and the internet form a big network that allows flowing data beyond the physical boundaries. Such easiness of communication and availabilityofelectronicdocumentincreasesthevolumeofdatawhichalsocreatedifficultyin the identification of original and relevantdata.

Chapter 3

CYBERCRIMES: MOBILE AND WIRELESS DEVICES

Course Outcomes

After successful completion of this module, students should be able to:

CO4	List out various Organizational security Policies and Measures in security issues of mobile computing domain	Remember

3.1 Introduction:

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

3.2 Proliferation of mobile and wireless devices:

- People hunched over their smartphones or tablets in cafes, airports, supermarkets and even at bus stops, seemingly oblivious to anything or anyone aroundthem.
- Theyplaygames,downloademail,goshoppingorchecktheirbankbalancesonthe go.

They might even access corporate networks and pull up a document or two on their mobile gadgets. Today,incredibleadvancesarebeingmadeformobiledevices.Thetrendisforsmallerdevices 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 powertorunsmallapplications,playgames andmusic,andmakevoicecalls.Akeydriverfor 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 belowhelpsusunderstandhowthesetermsarerelated.Letusunderstandtheconceptofmobile computing and the various types ofdevices.

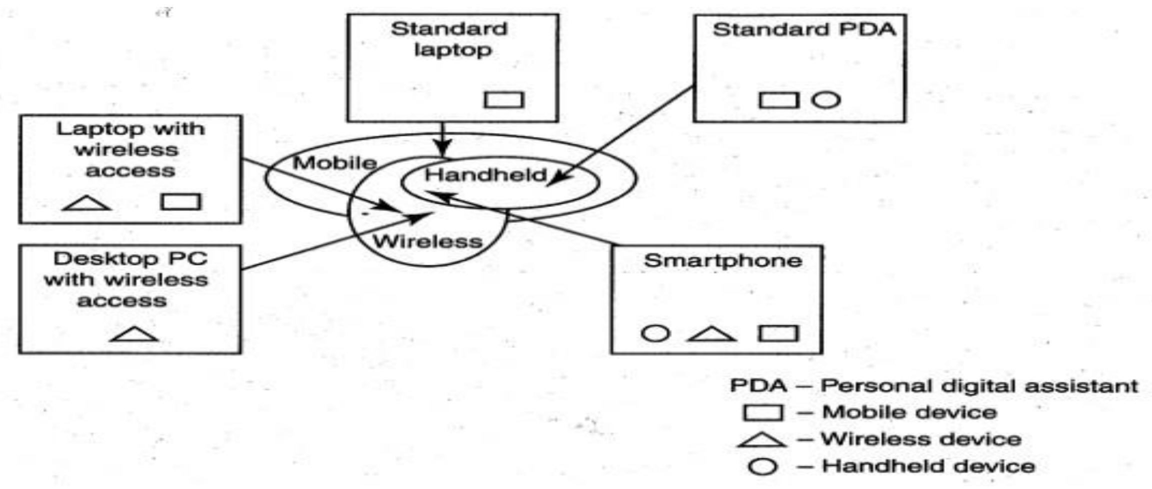


Fig 3.1: Mobile, Wireless and hand-held devices

Mobilecomputingis"takingacomputerandallnecessaryfilesandsoftwareoutintothefield." Many types of mobile computers have been introduced since 1990s. They are asfollows:

1. **Portable computer:** It is a general-purpose computer that can be easily moved from one placetoanother,butcannotbeusedwhileintransit,usuallybecauseitrequiressome"setting- up" and an AC power source.

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

3. **Internet tablet:** It is the Internet appliance in tablet form. Unlike a Tablet PC, the Internet tabletdoesnothavemuchcomputingpoweranditsapplicationssuiteislimited.Alsoitcannotreplace 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. **Personaldigitalassistant(PDA):**Itisasmall,usuallypocket-sized,computerwithlimited functionality. It is intended to supplement and synchronize with a desktop computer, giving access to contacts, address book, notes, E-Mail and otherfeatures.

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

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

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 Bluetoothcompatible.

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

3.3 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"fromAppleandGoogle-led"Android"phonesarethebestexamplesofthistrendand thereareplentyofotherdevelopmentsthatpointinthisdirection.Thissmartmobiletechnology 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.

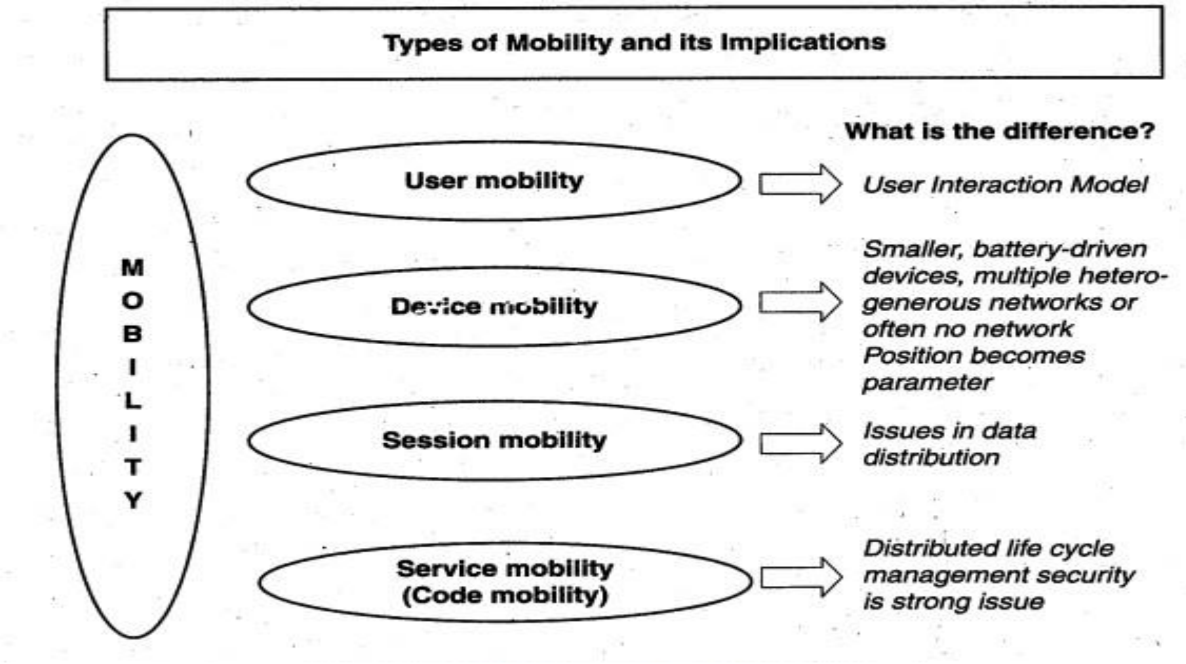

Types of Mobility and its Implications
What is the difference?
M O B I L I T Y
User mobility
User Interaction Model
Device mobility
Smaller, battery-driven devices, multiple hetero-generous networks or often no network Position becomes parameter
Session mobility
Issues in data distribution
Service mobility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

Fig 3.2 Mobility types and implications

Thenewtechnology3GnetworksarenotentirelybuiltwithIPdatasecurity.Moreover,IPdata worldwhencomparedtovoice-centricsecuritythreatsisnewtomobileoperators.Thereare numerous attacks that can be committed against mobile networks and they can originate from two primary vectors. One is from outside the mobile network - that is, public Internet, private networks and other operator's networks - and the other is within the mobile networks- that is, devices such as data-capable handsets and Smartphones, notebook computers or even desktop computers connected to the 3G network.

Popular types 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,2.5G2G,2.5G to 3G,3G, it is a growing need to educate the community people and provide awareness of such threats that exist while using mobile devices. Here are few examples of malware(s) specific to mobiledevices:

- **Skull Trojan:** I targets Series 60 phones equipped with the Symbian mobileOS.
- **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 vulnerablephoneitfindsthroughBluetoothWirelesstechnology.Theworstthingabout thiswormisthatthesourcecodefortheCabir-HandCabir-Ivirusesisavailableonline.

- **Mosquito Trojan:** It affects the Series 60 Smartphones and is a cracked version of "Mosquitos" mobile phonegame.
- **Brador Trojan:** It affects the Windows CE OS by creating a svchost. exe file in the Windowsstart-upfolderwhichallowsfullcontrolofthedevice.Thisexecutablefileis conductive to traditional worm propagation vector such as E-Mail fileattachments.
- **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 systemunavailable.Presently,oneofthemostcommoncybersecuritythreatstowiredInternet serviceproviders(iSPs)isadistributeddenial-of-service(DDos)attack.DDoSattacksareused to flood the target system with the data so that the response from the target system is either slowed orstopped.

3. Overbillingattack: Overbillinginvolvesanattackerhijackingasubscriber'sIPaddressand thenusingit(i.e.,theconnection)toinitiatedownloadsthatarenot"Freedownloads"orsimply 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 toconduct.

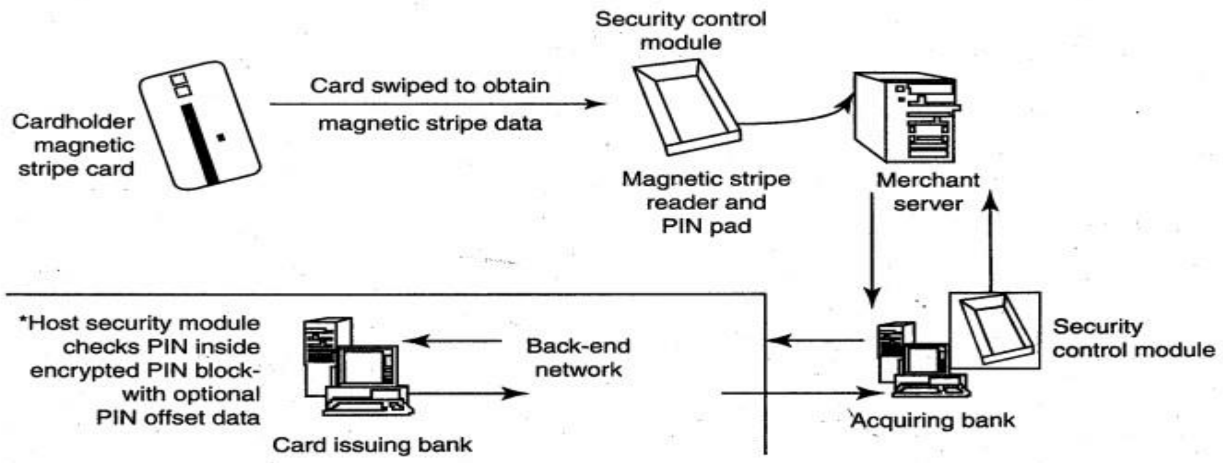
4. **Spoofedpolicydevelopmentprocess(PDP):**Theseofattacksexploitthevulnerabilitiesin the GTP [General Packet Radio Service (GPRS) TunnelingProtocol].

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 VolPsystems.

3.4 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 forcredit card processing too; wireless creditcard processing is arelatively 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.Itismostoftenusedbybusinessesthatoperatemainlyinamobileenvironment.

Fig 3.3 Online Environment for credit card transactions


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
Security control module
Card issuing bank
Acquiring bank

There is a system available from an Australian company "Alacrity" called closed-loop environment for forwireless (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 authorizedcardholder
3. The cardholder approves or rejects (passwordprotected)
4. The bank/merchant isnotified
5. The credit card transaction iscompleted.

3.5 Security Challenges Posed by Mobile Devices:

Mobility brings two main challenges to cybersecurity: first, on the hand-held devices, information is being taken outside the physically controlled environment and second remote access back to the protected environment is being granted. Perceptions of the organizations to these 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.

Asthenumberofmobiledeviceusersincreases,twochallengesarepresented:oneatthedevice 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 DirectoryAccessProtocol(LDAP)security,remoteaccessserver(RAS)security,mediaplayer control security, networking application program interface (API), securityetc.

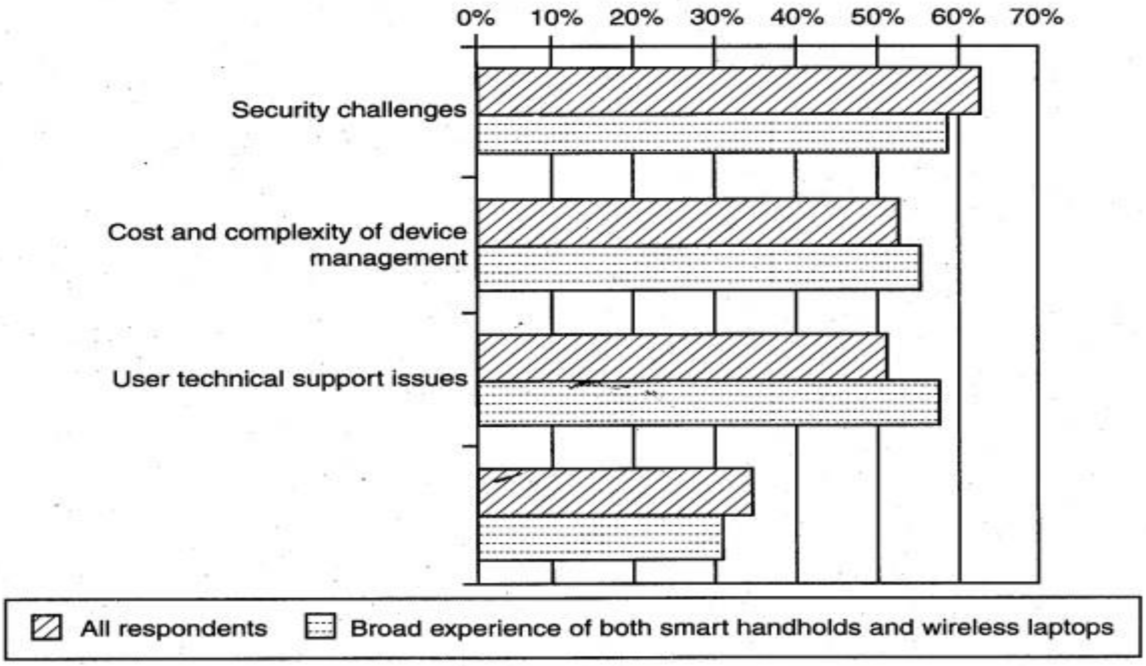


Fig 3.4 Important issues for managing mobile devices

3.6 REGISTRY SETTINGS FOR MOBILE DEVICES:

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

InadditiontosynchronizingwithaPC,ActiveSynccansynchronizedirectlywiththeMicrosoft 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 importantissuegiventheeasewithwhichvariousapplicationsallowafreeflowofinformation.

3.7 AUTHENTICATION SERVICE SECURITY:

Therearetwocomponentsofsecurityinmobilecomputing:securityofdevicesandsecurityin 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 play a crucial role in security of mobiledevices.

Someeminentkindsofattackstowhichmobiledevicesaresubjectedtoare:pushattacks,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.

3.8 ATTACKS ON MOBILE-CELL PHONES:

Mobile PhoneTheft:

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 hugesection 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)andWLANconnections.Therefore, unfortunately, the increased amount of freedom also offers more choices for viruswriters.

3.9ORGANIZATIONAL SECURITY POLICIES AND MEASURES IN MOBILE COMPUTING ERA:

Proliferation of hand-held devices used makes the cybersecurity issue graver than what we would tend to think. People have grown so used to their hand-helds they are treating themlike 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, mergerortakeoverplansandalsoothervaluableinformationthatcouldimpactstockvaluesin 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 contactinformation.

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. Organizationscan,however,reducetheriskthatconfidentialinformationwillbeaccessedfrom lost or stolen mobile devices through the followingsteps:

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

Organizational Policies for the Use of Mobile Hand-Held Devices

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

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

3.10 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 alsoposealargethreatastheyareportableWireless capabilityinthesedeviceshasalsoraised cybersecurityconcernsowingtotheinformationbeingtransmittedoverother,whichmakesit hard todetect.

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

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, physicalsecurity countermeasures are becoming very vital to protect the information on the employee's 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 otherconventionalsecuritycables.Oneendofthesecuritycableisfitintotheuniversalsecurity slotofthelaptopandtheotherendislockedaroundanyfixedfurnitureoritem,thusmakinga loop.Thesecablescomewithavarietyofoptionssuchasnumberlocks,keylocksandalarms.
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 itsdevicessuchasCD-ROMbays,PCMCIAcardsandHDDbayswhichcanbeeasilyremoved in the case of laptops protected by securitycables.
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. Alsoowingtotheirloudnature,theyhelpindeterringthieves.Modernsystemsforlaptopsare designed wherein the alarm device attached to the laptop transmits radio signals to a certain range around thelaptop.

4. **Warning labels and stamps:** Warning labels containing tracking information and identificationdetailscanbefixedontothelaptoptodeteraspiringthieves.Theselabelscannot be removed easily and are a low-cost solution to a laptop theft. These labels have an identification number that is stored in a universal database for verification, which, in turn makes the resale of stolen laptops a difficult process. Such labels are highly recommended for the laptops issued to top executives and/or key employees of theorganizations.

5. Other measures for protecting laptops are asfollows:

- Engraving the lapSStop with personaldetails
- Keeping the laptop close to oneself whereverpossible
- 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 andintrusion
- Updating the antivirus softwareregularly
- Tight office security using security guards and securing the laptop by locking it down in lockers when not inuse
- 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 theftdevice;
- 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 security and scanning forvulnerabilities.
4. Ensuring that unencrypted data/unprotected file systems do not posethreats.
5. Proper handing of removable drives/storage mediums /unnecessaryports.
6. Password protection through appropriate passwords rules and use of strongpasswords.
7. Locking down unwantedports/devices.
8. Regularly installing security patches andupdates.
9. Installing antivirus software/firewalls / intrusion detection system(IDSs).
10. Encrypting critical filesystems.

Chapter 4

CYBER SECURITY: ORGANIZATIONAL IMPLICATIONS

Course Outcomes

After successful completion of this module, students should be able to:

CO5	Demonstrate the cost of cybercrimes and IPR issues to detect and recover internal costs in an organization.	Understand

4.1 Organizational Implications

Introduction:

In the global environment with continuous network connectivity, the possibilities for cyberattacks can emanate from sources that are local, remote, domestic or foreign. They could be launched by an individual or a group. They could be casual probes from hackers using personal computers (PCs) in their homes, hand-held devices or intense scans from criminal groups.

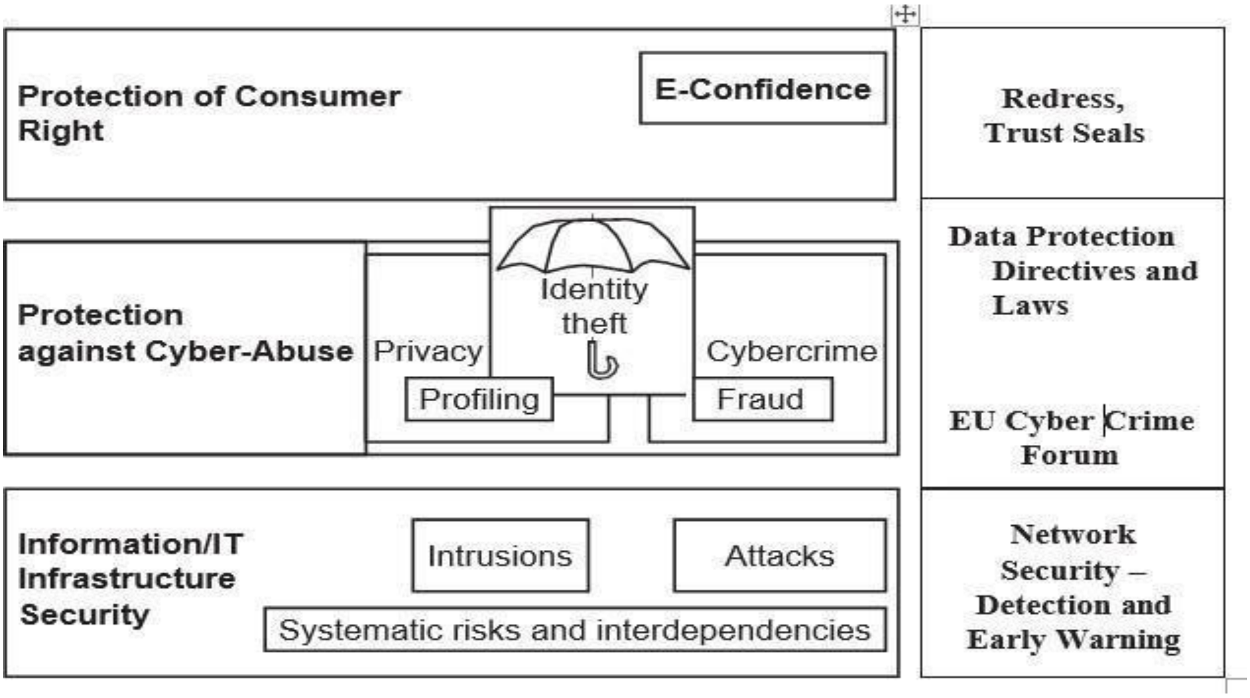

Protection of Consumer Right
E-Confidence
Redress, Trust Seals
Protection against Cyber-Abuse
Privacy
Identity theft
Cybercrime
Profiling
Fraud
Data Protection Directives and Laws
EU Cyber Crime Forum
Information/IT Infrastructure Security
Intrusions
Attacks
Systematic risks and interdependencies
Network Security – Detection and Early Warning

Fig 4.1: A cyber security perspective. EU is the European Union.

PI is information that is, or can be, about or related to an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual. Most information the organization collects about an individual is likely to come under “PI” category if it can be attributed to an individual. For an example, PI is an individual’s first name or first initial and last name in combination with any of the following data:

1. Social security number (SSN)/social insurancenumber.
2. Driver’s license number or identification cardnumber.
3. Bankaccountnumber,creditordebitcardnumberwithpersonalidentificationnumbersuch as an access code, security codes or password that would permit access to an individual’s financialaccount.
4. Home address or E-Mailaddress.

   Medical or healthinformation.

An insider threat is defined as “the misuse or destruction of sensitive or confidential information, aswellasITequipment thathousesthisdatabyemployees,contractorsandother ‘trusted’individuals.”

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

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

Insider Attack Example 1: Heartland Payment SystemFraud

A case in point is the infamous “Heartland Payment System Fraud” that was uncovered inJanuary2010.Thisincident bringsouttheglaringpointaboutseriousnessof“insiderattacks. In this case, the concerned organization suffered a serious blow through nearly 100 million credit cards compromised from at least 650 financial services companies. When a card is used to make a purchase, the card information is trans- mitted through a paymentnetwork.

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

Yet another incidence is the Blue Cross Blue Shield (BCBS) Data Breach in October 2009 the theft of 57 hard drives from a BlueCross BlueShield of Tennessee training facility puts the private in.formation of approximately 500,000 customers at risk in at least 32 states.

The two lessons to be learnt from this are:

1. Physical security is veryimportant.
2. Insider threats cannot beignored.

What makes matters worse is that the groups/agencies/entities connected with cybercrimesarealllinked.

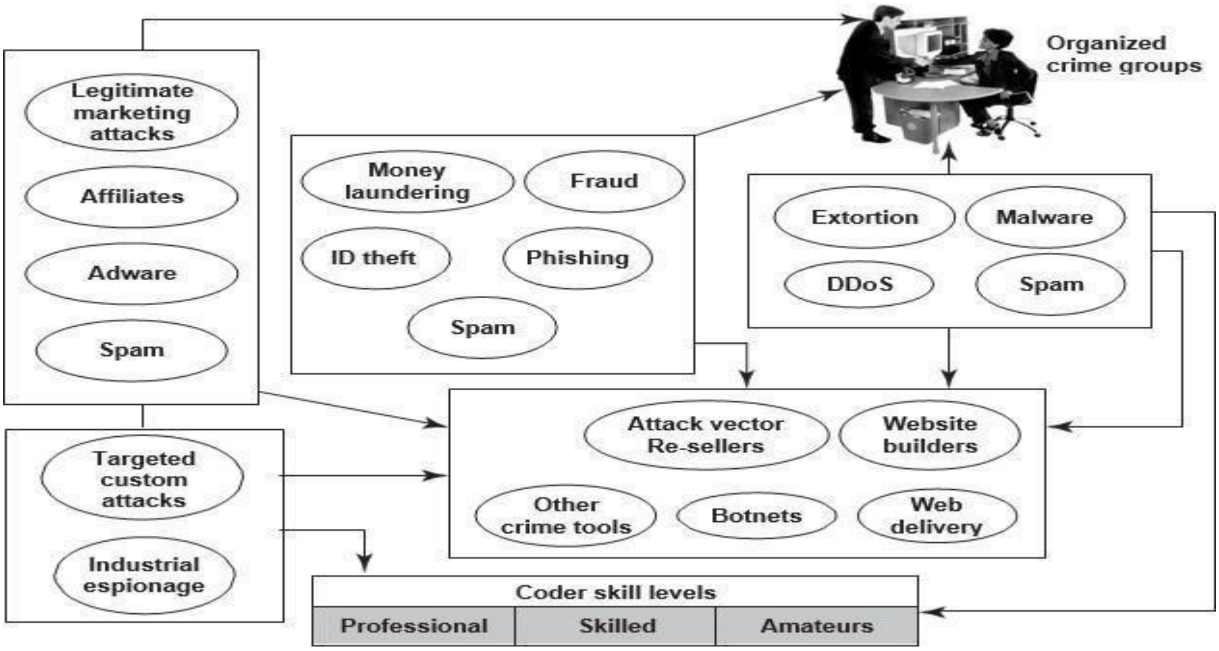


Fig: Cybercrimes – the flow and connections

There iscertainlyaparadigmshiftincomputingandworkpractices; with workforce mobility, virtual teams, social computing media, cloud computing services beingoffered,sharprise isnoticedinbusinessprocessoutsourcing(BPO)services,etc.

A key message from this discussion is that cybercrimes do not happen on their own or in isolation. Cybercrimes take place due to weakness of cybersecurity practices and “privacy” which may get impacted when cybercrimes happen.

Privacy has following four key dimensions:

1. **Informational/data privacy:** It is about data protection, and the users’ rights to determine how, when and to what extent information about them is communicated to otherparties.
2. **Personal privacy:** It is about content filtering and other mechanisms to ensure that the end-users are not exposed to whatever violates their moralsenses.

3. **Communication privacy:** This is as in networks, where encryption of data being transmitted isimportant.
4. **Territorial privacy:** It is about protecting users' property for example, the user devices from being invaded by undesired content such as SMS or E-Mail/Spam messages. The paradigm shift in computing brings many challenges for organizations; some such key challenges are describedhere.

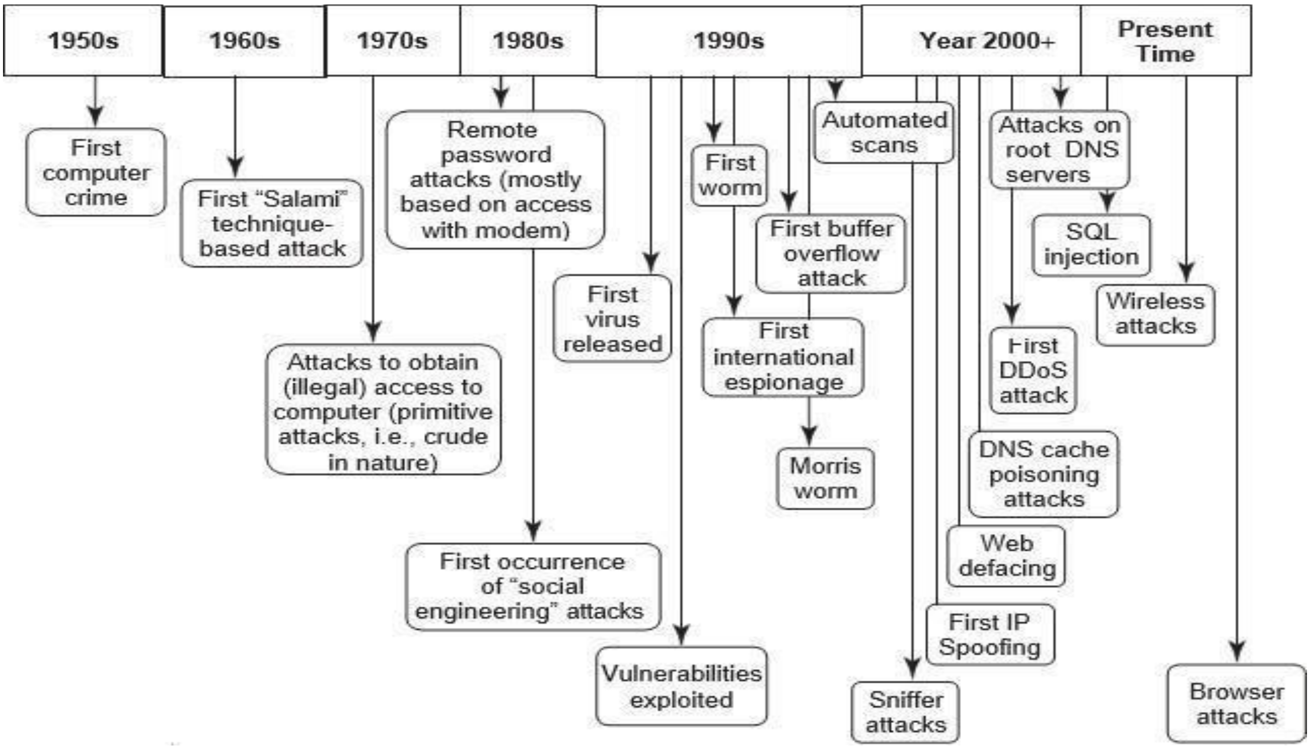

1950s
1960s
1970s
1980s
1990s
Year 2000+
Present Time
First computer crime
First "Salami" technique-based attack
Remote password attacks (mostly based on access with modem)
Attacks to obtain (illegal) access to computer (primitive attacks, i.e., crude in nature)
First occurrence of "social engineering" attacks
First virus released
Vulnerabilities exploited
First worm
Automated scans
First buffer overflow attack
First international espionage
Morris worm
Attacks on root DNS servers
SQL injection
Wireless attacks
First DDoS attack
DNS cache poisoning attacks
Web defacing
First IP Spoofing
Sniffer attacks
Browser attacks

Fig: Security threats – paradigm shift

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

1. **Industrial espionage:** There are several tools available for web administrators to monitorandtrackthevariouspagesandobjectsthatareaccessedontheirwebsite.
2. **IP-based blocking:** This process is often used for blocking the access of specific IP addresses and/or domainnames.
3. **IP-based"cloaking":**Businessesareglobalinnatureandeconomiesareinterconnected.
4. **Cyberterrorism:** "Cyberterrorism" refers to the direct intervention of a threatsource toward your organization'swebsite.

Confidential information leakage: "Insider attacks" are the worst ones. Typically, an organization is protected from external threats by your firewall and antivirus solutions.

Cost of Cybercrimes and IPR Issues: Lessons for Organizations

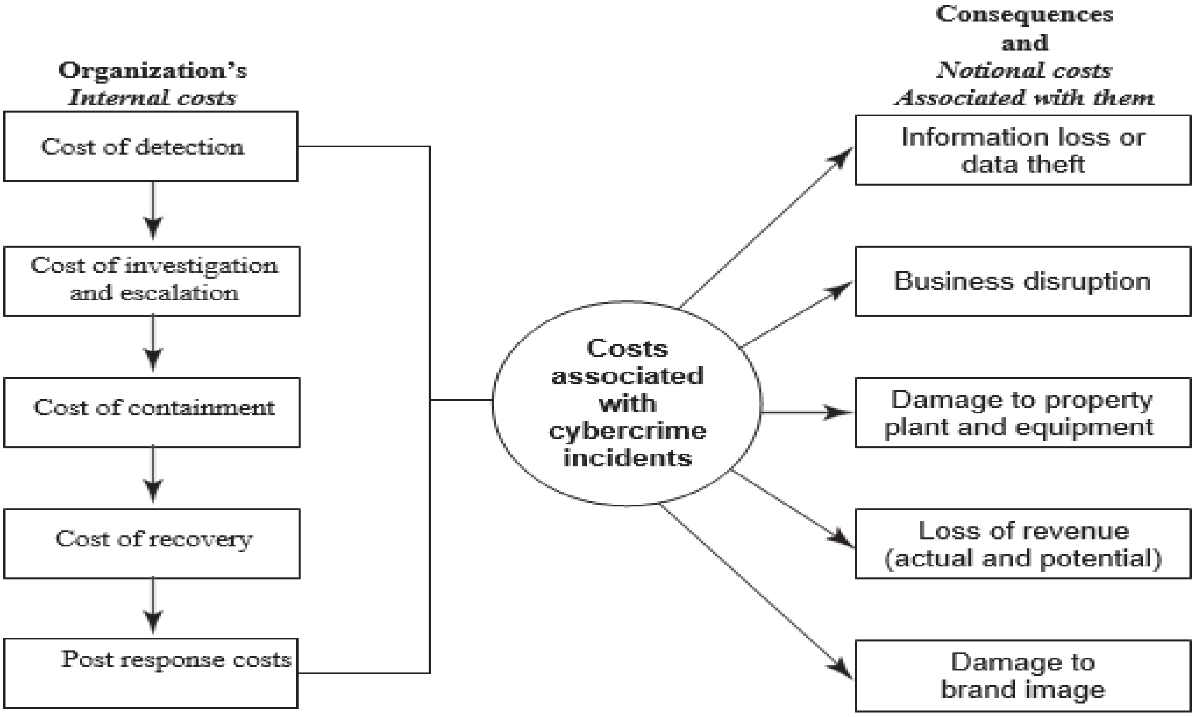

Organization's
Internal costs
Cost of detection
Cost of investigation and escalation
Cost of containment
Cost of recovery
Post response costs
Costs associated with cybercrime incidents
Consequences and Notional costs Associated with them
Information loss or data theft
Business disruption
Damage to property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

Fig: Cost of cybercrimes

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

Detection and recovery constitute a very large percentage of internal costs. This is supportedbya benchmarkstudyconductedbyPonemonInstituteUSAcarriedoutwiththesample of 45 organizations representing more than 10 sectors and each with a head count of at least 500 employees.

- **Organizations have Internal Costs Associated with Cyber securityIncidents**

  Theinternalcoststypicallyinvolvepeoplecosts,overheadcostsandproductivitylosses. The internal costs, in order from largest to the lowest and that has been supported by the benchmark studymentioned:

  1. Detectioncosts (25%)
  2. Recoverycosts (21%)
  3. Post responsecost (19%)
  4. Investigationcosts (14%)
  5. Costs of escalation and incidentmanagement (12%)
  6. Cost ofcontainment (9%)

- **The consequences of cybercrimes and their associated costs,mentioned**

  1. Information loss/datatheft.(42%)
  2. Business disruption.(22%)
  3. Damages to equipment, plant andproperty.(13%)
  4. Loss of revenue and brandtarnishing.(13%)

5. Othercosts.(10%)

- **The impact on organizations by various cybercrimes**

1. Virus, worms andTrojans-100%
2. Malwares-80%
3. Botnets-73%
4. Web basedattacks-53%
5. Phishing and Social engineering-47%
6. Stolendevices-36%
7. Maliciousinsiders-29%
8. Maliciouscode-27%

- **Average days taken to resolve cyberAttacks**

1. Attacks by Malicious insiders-4days
2. Malicious code-39days
3. Web based attacks-19days
4. Data lost due to stolen devices-10days
5. Phishing and social engineering attacks-9 days
6. Virus,worms,and trojans-2.5days
7. Malware-2days
8. Botnets- 2 days

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

Again, there are lessons to learn:

1. **Endpoint protection:** It is an often-ignored area but it is IP-based printers, although they are passive devices, are also one of theendpoints.
2. **Securecoding:**Thesepracticesareimportant becausetheyareagoodmitigationcontrolto protect organizations from "Malicious Code" inside businessapplications.
3. **HR checks:** These are important prior to employment as well as afteremployment.
4. **Access controls:** These are always important, for example, shared IDs and sharedlaptops are dangerous.
5. **Importanceofsecuritygovernance:**Itcannotbeignoredpolicies,proceduresandtheir effective implementation cannot beover-emphasized.

- **Organizational Implications of SoftwarePiracy**

Use of pirated software is a major risk area for organizations.

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

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

1. Pirated software is cheaper and more readilyavailable.
2. Many others use pirated softwareanyways.
3. Latest versions are available faster when pirated software isused.

4.3 Web Threats for Organizations: The Evils and Perils

Internetandthe Webisthe wayofworkingtodayintheinterconnecteddigitaleconomy. More and more business applications are web based, especially with the growing adoption of cloudcomputing.

- **Overview of Web Threats toOrganizations**

The Internet has engulfed us! Large number of companies as well as individuals have a connection to the Internet. Employees expect to have Internet access at work just like 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.

- **Employee Time Wasted on InternetSurfing**

This is a very sensitive topic indeed, especially in organizations that claim to have a "liberal culture." Some managers believe that it is crucial in today's business world to have the finger on the pulse of your employees.

People seem to spend approximately 45-60 minutes each working day on personal web surfing at work.

- **Enforcing Policy Usage in theOrganization**

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

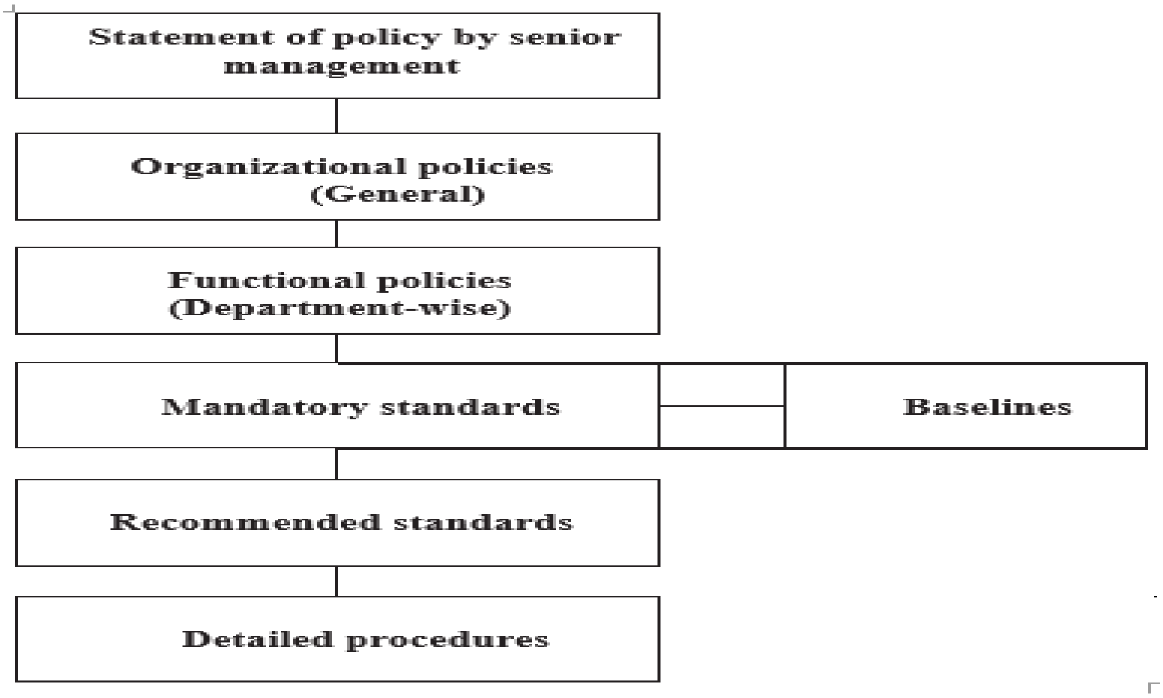

Statement of policy by senior management
Organizational policies (General)
Functional policies (Department-wise)
Mandatory standards
Baselines
Recommended standards
Detailed procedures

Fig4.1 : Policy hierarchy chart

- **Monitoring and Controlling Employees' InternetSurfing**

A powerful deterrent can be created through effective monitoring and reporting of employees' Internet surfing.
Even organizations with restrictive policies can justify a degree of relaxation; for example, allowing employees to access personal sites only during the lunch hour or during specified hours.

- **Keeping Security Patches and Virus Signatures Up toDate**

Updating security patches and virus signatures have now become a reality of life, a necessaryactivityforsafetyinthecyberworld!Keepingsecuritysystemsuptodatewithsecurity signatures, software patches, etc. is almost a nightmare formanagement.

- **Surviving in the Era of LegalRisks**

As website galore, most organizations get worried about employees visiting inappropriate or offensive websites. We mentioned about Children's Online Privacy Protection.
Serious legal liabilities arise for businesses from employee's misuse/inappropriate use of the Internet.

- **Bandwidth WastageIssues**

Today's applications are bandwidth hungry; there is an increasing image content in messages and that too, involving transmission of high-resolution images.

There are tools to protect organization's bandwidth by stopping unwanted traffic before it even reaches your Internet connection.

- **Mobile Workers Pose SecurityChallenges**

Use of mobile handset devices in cybercrimes. Most mobile communication devices for example, the personal digital assistants has raised security concerns with their use. Mobile workers use those devices to connect with their company networks when they move. So the organizations cannot protect the remote user system as a result workforce remains unprotected. We need tools to extend web protection and filtering to remote users, including policy enforcement

- **Challenges in Controlling Access to WebApplications**

Today, a large number of organizations' applications are web based. There will be more in the future as the Internet offers a wide range of online applications, from webmail or through social networking to sophisticated business applications. Employees use personal mail id to send business sensitive information (BSI) for valid or other reasons. It leads to data security breach. The organizations need to decide what type of access to provide to employees.

- **The Bane ofMalware**

Many websites contain malware. Such websites are a growing security threat. Although most organizations are doing a good job of blocking sites declared dangerous, cyber attackers, too, are learning. Criminals change their techniques rapidly to avoid detection.

- **The Need for Protecting Multiple Offices andLocations**

Delivery from multi-locations and teams collaborating from multi-locations to deliver a single project are a common working scenario today. Most large organizations have several offices at multiple locations. In such scenario Internet-based host service is best idea to protect many locations.

4.4 Security and privacy implications from cloud computing

Cloud computing is one of the top 10 Cyber Threats to organizations. There are data privacy risks through cloud computing. Organizations should think about privacy scenarios in terms of "user spheres". There are three kinds of spheres and theircharacteristics:

1.User sphere: Here data is stored on users' desktops, PCs, laptops, mobile phones, Radio Frequency Identification (RFID) chips, etc. Organization's responsibility is to provide access to users and monitor that access to ensure misuse does nothappen.
2.Recipient sphere: Here, data lies with recipients: servers and databases of network providers, serviceproviders or other parties with whom data recipient shares data. Organizations responsibility is to minimize users privacy risk by ensuring unwanted exposure of personal data of users does nothappen
3.Joint sphere: Here data lies with web service provider's servers and databases. This is the in between sphere where it is not clear to whom does the data belong. Organization responsibility is to provide users some control over access to themselves and to minimize users futures privacyrisk.

4.5 Social Media Marketing: Security Risks and Perils for Organizations

Social media marketing has become dominant in the industry. According to fall 2009 survey by marketing professionals; usage of social media sites by large business-to-business (B2B) organizations shows the following:

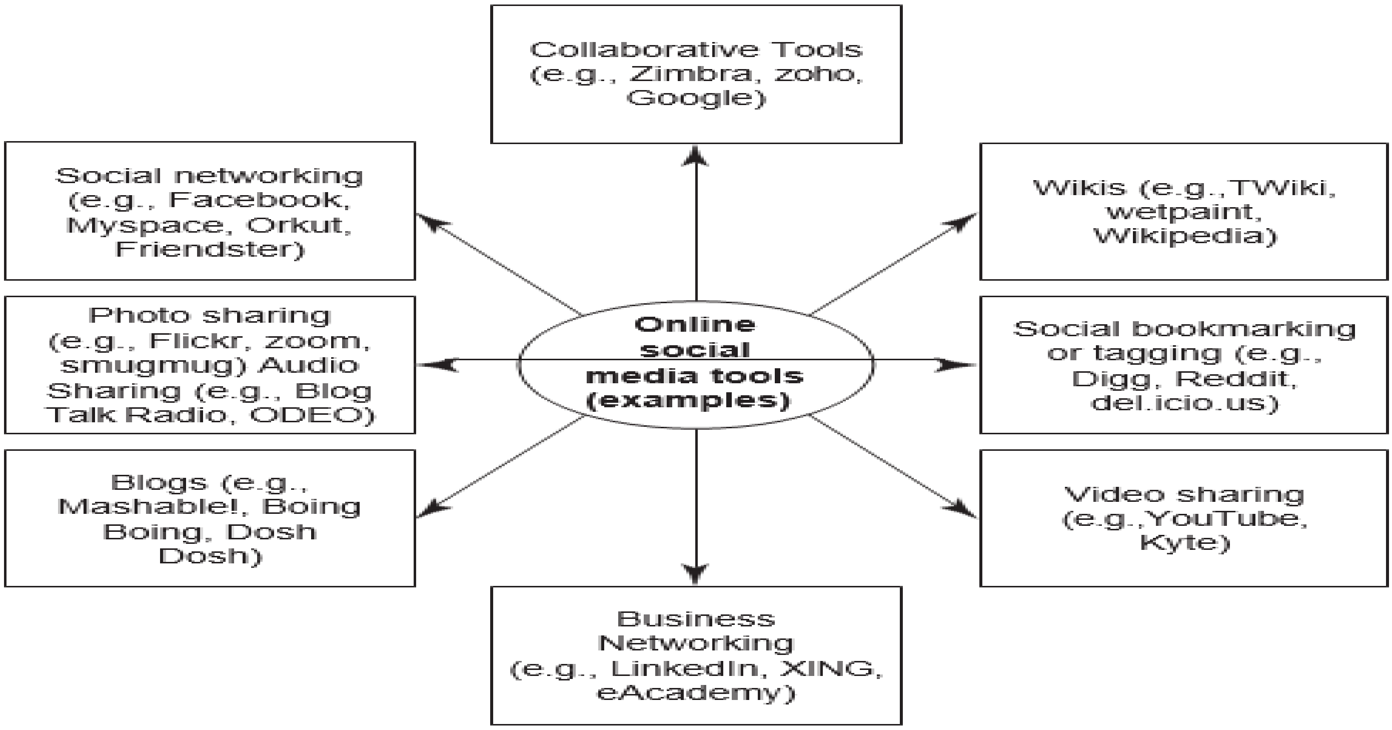

Collaborative Tools (e.g., Zimbra, zoho, Google)
Social networking (e.g., Facebook, Myspace, Orkut, Friendster)
Wikis (e.g.,TWiki, wetpaint, Wikipedia)
Photo sharing (e.g., Flickr, zoom, smugmug) Audio Sharing (e.g., Blog Talk Radio, ODEO)
Online social media tools (examples)
Social bookmarking or tagging (e.g., Digg, Reddit, del.icio.us)
Blogs (e.g., Mashable!, Boing Boing, Dosh Dosh)
Video sharing (e.g.,YouTube, Kyte)
Business Networking (e.g., LinkedIn, XING, eAcademy)

FIG: Social Media Marketing Tools

1. Facebook is used by 37% of theorganizations.
2. LinkedIn is used by 36% of the organizations.
3. Twitter is used by 36% of theorganizations.
4. YouTube is used by 22% of theorganizations.
5. My Space is used by 6% of theorganizations.

Although the use of social media marketing site is rampant, there is a problem related to “social computing” or “social media marketing” – the problem of privacy threats. Exposures to sensitive PI and confidential business information are possible if due care is not taken by organizations while using the mode of “social mediamarketing.”

• Understanding Social MediaMarketing

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

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

1. To be able to reach to a larger target audience in a more spontaneous and instantaneous manner without paying large advertisingfees.
2. Toincreasetraffictotheirwebsitecomingfromothersocialmediawebsitesbyusing Blogsand social and business-networking. Companies believe that this, in turn, may increase their “page rank” resulting in increased traffic from leading search engines.
3. To reap other potential revenue benefits and to minimize advertising costs because social media complements other marketing strategies such as a paid advertisingcampaign.
4. To build credibility by participating in relevant product promotion forums and responding topotential customers’ questions immediately.

5. To collect potential customer profiles. Social media sites have information such asuserprofile data, which can be used to target a specific set of users foradvertising.

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

1. Twitter is used with higher priority to reach out to maximum marketers in the technology space and monitor thespace.
2. Professional networking tool LinkedIn is used to connect with and create a community of top executives from the Fortune500.
3. Facebook as the social group or social community tool is used to drive more traffic to Websense website and increase awareness aboutWebsense.
4. YouTube(thevideocapabilitytooltorundemonstrationsofproducts/services,etc.) isused to increase the brand awareness and create a presence for corporatevideos.
5. Wikipedia is also used for brand building and drivingtraffic.

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

4.6 Social Computing and associated challenges fororganizations:

- Social computing is also known as “web 2.0”
- It empowers people to use web based public products and services.
  It helps thousands of people to across the globe to support their work, health learning, getting citizenship tasks in a number of innovative ways.
- In this process, a lot of information gets exchanged and some of that could be confidential, personally identifiable information(PII) etc,. This could be gold mine for the cyber criminals.
- Getting too used to readily available information, people may get into the mode of not questioning the accuracy and reliability of information that they readily get on the internet.
- With social computing, there are new threats emerging, those threats relate to security, safety, and privacy.

Chapter 5

CYBERCRIME: EXAMPLES AND MINI-CASES EXAMPLES

Course Outcomes

After successful completion of this module, students should be able to:

CO5	Translate the cost of cybercrimes and IPR issues to detect and recover a very large percentage of internal costs	Understand

5.1 OFFICIAL WEBSITE OF MAHARASHTRA GOVERNMENT HACKED:

SEP 19, 2007 09:38:52 IST

The official website of the Maharashtra government was allegedly hacked, forcing the state Information Technology department to lodge a formal complaint with the city police on Tuesday. The website was hacked for the second time in the past two weeks, the fourth since July. The previous attack took place on September 5.

Joint Commissioner of Police (Crime) Rakesh Maria said that access to the website, www.maharashtra.gov.in , had been blocked for a while. "It had some Arabic content posted on it by the hacker. The IT department has lodged an FIR with the police and we will try and trace the culprit," said Maria. It is suspected that the same group of international hackers was behind all the four attacks.

The site was hacked into late on Monday night by a person or a group calling itself "cool hacker" who had left an imprint of a hand on the website. The state's information and technology department came to know of the hacking Tuesday morning and immediately blocked all access to the website.

State officials maintained that no data had been lost and no serious damage had been inflicted on the website, which is updated daily with information on various government regulations and decisions, and supports links to all government departments. The hacker could only manage to damage the homepage. However, restoration work is in progress.

The state government website is hosted on a VSNL server. In the month of August, 345 Indian websites — ending with .in, .co.in and edu.in — were defaced by hackers. Nearly 2,700 Indian websites have been hacked since January.

5.2 Indian Banks Lose Millions of Rupees:

MUMBAI, Aug 14 (Reuters) - Cyber criminals hacked the systems of India's Cosmos Bank and siphoned off nearly 944 million rupees ($13.5 million) through simultaneous withdrawals across 28 countries over the weekend, the bank has told police.

The co-operative bank said unidentified hackers stole customer information through a malware attack on its automated teller machine (ATM) server, withdrawing 805 million rupees in 14,849 transactions in just over two hours on Aug. 11, mainly overseas.

Apart from the ATM withdrawals, the hackers transferred 139 million rupees to a Hong Kong-based company's account by issuing three unauthorised transactions over the SWIFT global payments network, the bank said in a police complaint, a copy of which was seen by Reuters.

SWIFT, whose messaging system is used to transfer trillions of dollars a day, said it did not comment on individual cases.

Cosmos Bank, based in the western city of Pune, said in a press statement that its main banking software receives debit card payment requests via a "switching system" but it was bypassed in the attack.

“During the malware attack, a proxy switch was created and all the fraudulent payment approvals were passed by the proxy switching system,” the bank said. The bank declined to reveal the countries, citing security risks. Police said they were investigating the theft. A police official, who declined to be named, said they had enlisted the help of experts to find out how authorised transactions were conducted simultaneously in various countries. India’s City Union Bank Ltd reported in February that it had suffered three “fraudulent remittances” of nearly $2 million that had been pushed through the SWIFT financial platform.

In 2016, unknown hackers stole more than $81 million from the Bangladesh central bank’s account with the Federal Reserve Bank Of New York. Investigators have made little progress in the case.

“While there is growing awareness to regularly update an organisation’s cyber preparedness and defence mechanisms, a large number of institutions wake up to this reality only post an incident which often leads to a loss of reputation and/or financial misappropriation,” said Nikhil Bedi, a partner with Deloitte India.

5.3 PARLIAMENT ATTACK:

Australia's security agencies are investigating a cyber-breach of the Federal Parliament's computer network that the ABC understands is likely the result of a foreign government attack. The agencies are looking into whether China is behind the incident.

In a statement, Federal Parliament's presiding officers said authorities were yet to detect any evidence data had been stolen in the breach. One source said the response to the attack had been swift but the hackers were "sophisticated this time around". Computer passwords have been reset as a precaution as the investigations continue. "We have no evidence that this is an attempt to influence the outcome of parliamentary processes or to disrupt or influence electoral or political processes," the Parliament's presiding officers said in a statement. "Accurate attribution of a cyber-incident takes time and investigations are being undertaken in conjunction with the relevant security agencies." The Australian Signals Directorate (ASD) is working to secure the network and says action was taken as soon as the breach was detected.

"The necessary steps are being taken to mitigate the compromise and minimise any harm," ASD said in a statement. A cyber security expert warned about the seriousness of the breach. "If you look at what goes on in Parliament House, you've got politicians, you've got staffers, you've got government departments that are moving in and out of the organisation and a lot of that is through electronic means," adjunct professor Nigel Phair, from the University of Canberra, said.

"If I was a nation state, or dare I say any hacker looking for state secrets, this is the crown jewels."

Prime Minister Scott Morrison said no Federal Government departments or agencies had been targeted in the attack. But he refused to offer details on the breaches at Parliament House.

"I don't propose to go into any sort of detailed commentary on the source or nature of this," Mr Morrison said. "Once further information is available then we will be in a position to provide further detail."

Hackers caught in early stages, ABC told, Sources have told the ABC that the hackers were caught in the early stages of gaining access to the computer network. The incident has been compared to a robber breaking into a house, whereby authorities know the front door has been broken but are yet to find out if anything else has been taken, or if there is another way to break in. The attack does not affect the computer systems of government ministers and their staff, however it does affect government backbenchers, the Opposition and crossbenchers.

Labour politicians and staff said access to their emails had been intermittent since the attack. Opposition Leader Bill Shorten said he was satisfied with the response so far. "I've had some briefings on it. I'm satisfied from what I've heard initially that our security agencies and the president [of the Senate] and the Speaker [of the House] have moved in the right way to make sure that our parliamentary networks are secure," he said. Mr Shorten described the breach as a "wake up call", saying while Parliament had the resources to respond to a cyber attack, many small and medium-sized businesses did not. "They don't have the budget of the Parliament of Australia. If I'm prime minister I'm going to invest a lot more in the cyber security of our small and medium sized enterprises."

Key points:

- Authorities are yet to uncover any evidence that data was stolen in the breach.
- Computer passwords were reset as a precaution as investigations continue.
- The hackers were caught in the early stages of gaining access to the system.

5.4 PUNE CITY POLICE BUST NIGERIAN RACKET:

Police team from PimpriChinchwad Police Social Security Cell (SSC) in Maharashtra's Pune have busted a massive sex racket and rescued 12 Nigerian girls forced into prostitution. Four Nigerian women were arrested during the raid conducted on Tuesday night, February 2, for allegedly running the prostitution racket.

Police said they had received information about foreigners operating prostitution racket from Vakratund building in Omkar Colony in Morya Park, Pimple Gurav, under the Sangvi police station. Acting on the tip-off, four men acting as decoy customers visited the apartment and found that a prostitution racket was being run from there by Nigerian nationals.

Accordingly, SSC's Senior Police Inspector VitthalKubde formed a team with police officers Assistant Police Inspector NileshWaghmare and Police Sub Inspector DhairyasheelSolanke to investigate the case.
A raid was conducted and 16 Nigerian women were taken into police custody during the raid, of which 12 were released. Valuables worth Rs 82,920 was seized from their possession during the raid. "For the past 20 days, the social security cell had been working on the tip-off. After collecting concrete information, on Tuesday night we sent four decoy customers to the flat in Pimple Gaurav. We planned the raid after getting confirmation from the decoys," an official told journalists.

The 12 rescued Nigerian women have been sheltered at the Rescue Foundation in Hadapsar, Pune after medical examination. The police are verifying the passports and visas of the women and further investigation is underway. The action was taken under the guidance of Commissioner of Police Krishna Prakash, Additional Commissioner of Police RamnathPokale, and Deputy Commissioner of Police (Crime) SudhirHiremath by a team led by ACP PrernaKatte and Senior Police Inspector Kubde.

5.5 E-mail spoofing instances:

Email spoofing is the act of sending emails with **a forged sender address**. It tricks the recipient into thinking that someone they know or trust sent them the email. Usually, it's a tool of a phishing attack, designed to take over your online accounts, send malware, or steal funds.

Spoofed email messages are easy to make and easy to detect. However, more malicious and targeted varieties can cause significant problems and pose a huge security threat.

Reasons for email spoofing

The reasons for email spoofing are quite straightforward. Usually, the criminal has something malicious in mind, like stealing the private data of a company.

Here are the most common reasons behind this malicious activity:

- **Phishing.** Almost universally, email spoofing is a gateway for phishing. Pretending to be someone the recipient knows is a tactic to get the person to click on malicious links or provide sensitive information.
- **Identity theft.** Pretending to be someone else can help a criminal gather more data on the victim (e.g. by asking for confidential information from financial or medical institutions).
- **Avoiding spam filters.** Frequent switching between email addresses can help spammers avoid being blacklisted.
- **Anonymity.** Sometimes, a fake email address is used to simply hide the sender's true identity.

Dangers of email spoofing

Email spoofing is incredibly dangerous and damaging because it doesn't need to compromise any account by bypassing security measures that most email providers now implement by default. It exploits the human factor, especially the fact that no person double-checks the header of every email that they receive. Besides, it's incredibly easy for attackers and requires almost no technical know-how to do it on a basic level. Not to mention the fact that every mail server can be reconfigured to be identical or almost identical to slip by.

5.6 The Indian Case of online Gambling:

Since it is not possible to prevent Internet gambling completely, effectively regulating it remains the only viable option. India can learn from the experience of several countries that have successfully regulated online gambling.

Gambling is prohibited in India. The Public Gambling Act, 1867 and several local acts passed by the states make it a legally proscribed activity with punishments ranging from financial fines to years of imprisonment. Despite these laws, the Federation of Indian Chambers of Commerce and Industry (FICCI) estimates India's illegal bettingmarket at more than Rs 3,00,000 crore, which is about the size of India's defence budget as of 2019. This amount exceeds the total amount India spends on agriculture, education and health by $10 billion or Rs 7.5 thousand crore.

The CBI's report on 'cricket match fixing and related malpractices' talks of the emergence of betting syndicates and cartels, run on ground by bookies and punters, and hints at the involvement of the underworld. That was almost 20 years back, and betting on any One-Day International match anywhere in the world ran into hundreds of crores, according to the report. Today, betting has gone online, with neat interfaces, embedded payment systems, dashboards to calculate odds, alert notifications and mobile applications.

There is a certain ambiguity about the application of gambling statutes to the online space as the laws are more suited to act upon a physical gaming house and related instrumentalities. Complicating this situation is the designation of certain games as 'games of skill' where "success depends principally upon the superior knowledge, training, attention, experience and adroitness of the player" and players can transact, bet and exchange monies playing the same. It is essential to disambiguate the policy conundrum around gambling especially in the online space as this can be utilised as an opportunity for harm prevention as well as possible gains in revenue.

5.7 An Indian Case of Intellectual Property Crime:

Engagement with India on Intellectual Property Rights (IPR) continues, primarily through the Trade Policy Forum's Working Group on Intellectual Property. In 2016, India released its comprehensive National IP Policy, with its primary focus being on awareness and building administrative capacity. The portfolio of Copyright and Semi-Conductors shifted to the Department of Industrial Policy and Promotion, Ministry of Commerce, which was subsequently renamed as the Department of Promotion of Industry and Internal Trade (DPIIT). Under DPIIT, a Cell of IP Promotion and Management (CIPAM) was set up and is tasked with implementing the IP Policy and interagency coordination. However, their focus appears to be awareness building amongst citizens. In 2017, CIPAM conducted the first ever all India enforcement workshop for police officers and launched a toolkit for police to enforce IP rights. Post this initiative, the Ministry of Home Affairs announced that IP would become a mandatory subject for all police training academies.

In 2016, the state of Telangana set up India's first IP Crime Unit, to combat the menace of internet piracy. In 2017, Maharashtra followed suit by setting up the Digital Crime Unit (MCDCU) and has taken down many sites that carry infringing content. The MCDCU is the first public private partnership unit for the law enforcement agency in all of India. As of 2019, they have blocked over 250 sites that carry predominately infringing content. In 2018, Mizoram became the third state to announce the setting up of a Digital Crime Unit to combat digital fraud and copyright theft.

In 2016, the Indian Patent Office (IPO) hired 458 examiners to address the issue of patent and trademark backlog. In 2017, the Patent Rules and the Trademark Rules were revised, to include strict timelines to dispose of cases and streamline examination. Special discounts for filing and an expedited examination for start-ups was introduced. With the hiring of these examiners and these initiatives, the wait-times at the Indian Patent Office were reduced. In 2019, the IPO released draft Copyright Rules and a second Patent Rules Amendment - these are under consideration and yet to be finalized.

5.8 Financial Frauds in Cyber Domain:

A small, rural hospital contracted with an emergency medical group for emergency department (ED) coverage. The group was paid monthly by EFT from the hospital's account to the ED group's account. In June, the hospital received an email invoice from the ED group with instructions to send payment to a new account. The hospital sent the $200,500 payment to the new account on July 10. On July 12, the payment was returned because the new account was frozen. On July 16, the ED group emailed new account information and instructions to the hospital. The hospital sent the $200,500 payment to the new account.

In early August, the ED group sent the next monthly invoice by email with instructions to send the funds to another new account. The hospital sent the $206,500 payment on August 13. It was later discovered that the requests to send the funds to the new accounts were fraudulent. The ED group never sent the emails requesting EFT account changes. The cyber criminals who sent the fraudulent emails and set up the accounts ended up collecting $407,000 from the hospital. When the hospital discovered that the money had been sent to an invalid account, the loss was reported to the hospital's insurance agent and cyber liability carrier. The hospital was advised to take the following steps:

1. File a complaint with the local police department.
2. Submit a complaint to the FBI's Internet Crime Complaint Center (IC3).
3. Contact the bank's fraud department to flag the transactions as fraudulent.
4. Contact the local FBI office.

After the incident, the hospital began using the following fraud prevention measures.

1. A change in policy that requires all wire transfer procedures to have oral confirmation from vendors and contractors if there are any changes in payment instructions.
2. Managers are now required to send emails using two-step account verification procedures.

3. Employees in the IT, Finance, and Revenue Cycle Departments attend required training on cyber security and cyber fraud risks.

Risk management considerations:

Social engineering typically involves a hacker using a compromised business email account to request money, passwords, banking information, or personally identifying information from the holder of the compromised account. The victim is deceived into thinking the request is from a legitimate source, such as a friend or a financial institution with whom the victim has a business relationship.

In this case, the hospital fell victim to a social engineering fraud through a phishing email. The compromised ED group email requested money through multiple wire transfers, tricking the hospital into sending $407,000.

The following practices can help combat phishing attacks.

1. Be suspicious of emails from unknown sources, especially those requesting sensitive information or stressing the urgency and importance of the request.
2. Train employees to recognize suspicious emails and forward them to someone who manages cyber security.
3. Establish an incident response plan to initiate in case a phishing attack is successful.
4. Use technology to detect and test emails for malicious content.
5. Require multifactor authentication.
6. Conduct regular security training for employees and provide testing to ensure understanding.
7. Follow your instincts, and always report suspicious.

We have provided illustrations of banking frauds (including credit card-related crimes), online gambling, IPR crimes, digital media piracy, hacking, computer frauds, website attacks, counterfeit hardware, malicious use of the Internet, social networking victims, etc.

List of illusions in Financial Frauds in Cyber Domain:

Illusion number:	Title	Topic
1.	Stolen Credit Card Information	Phishing and credit card frauds (banking frauds)
2.	Phishing Incidence	Phishing (credit card frauds)
3.	Online Credit Card Theft Ring	Credit Card Frauds
4.	Understanding Credit Card Fraud Scenarios	Credit Card Frauds
5.	ShadowCrew – The Internet Mafia Gang	Credit Card Frauds
6.	Dirty Relations – Goods Delivery Fraud	Frauds from online purchasing
7.	Fake Mails Promising Tax Refunds: Beware	Internet banking
8.	Phone Scam Targets Your Bank Account	DoS(denial-of-service)

Bibliography

1. Bauer, Johannes M. and Van Eeten, Michel J. G(2009)- Cybersecurity: Stakeholder Incentives, Externalities, and Policy Optins.
2. Anderson, Ross J (2008)- Security Engineering
3. Anderson, Ross J (2008)- Security Economics and the Internal Market
4. Bellovin, Steven M (2009) – The Governament and Cybersecurity