There are some important cyber security policies recommendations describe below-

Virus and Spyware Protection policy:

- It helps to detect threads in files, to detect applications that exhibits suspicious behavior.
- Removes, and repairs the side effects of viruses and security risks by using signatures.

Firewall Policy:

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

Intrusion Prevention policy:

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

Application and Device Control:

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

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 cyber frauds:

Forgery (Section 464)

Forgery pre-planned for cheating (Section 468)

False documentation (Section 465)

Presenting a forged document as genuine (Section 471)

Reputation damage (Section 469)

Companies Act of 2013

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

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

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

NIST Compliance

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

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

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

Unit 3

CYBERCRIMES: MOBILE AND WIRELESS

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

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 around them.
- They play games, download email, go shopping or check their bank balances on the go.

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

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

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

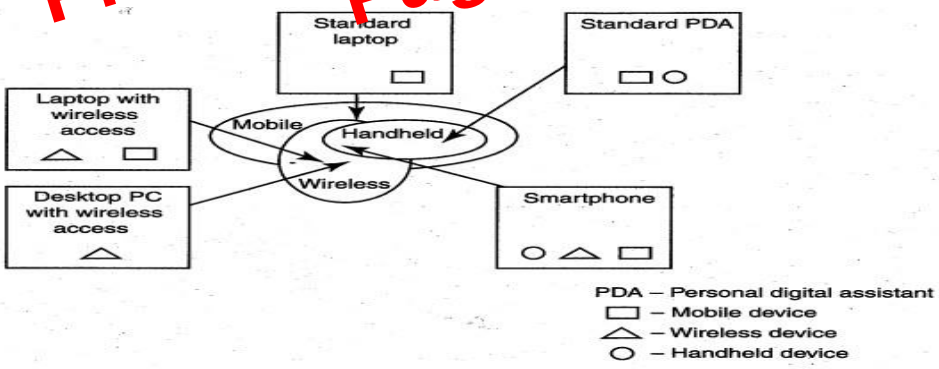

Figure : Mobile, Wireless and hand-held Devices

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

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

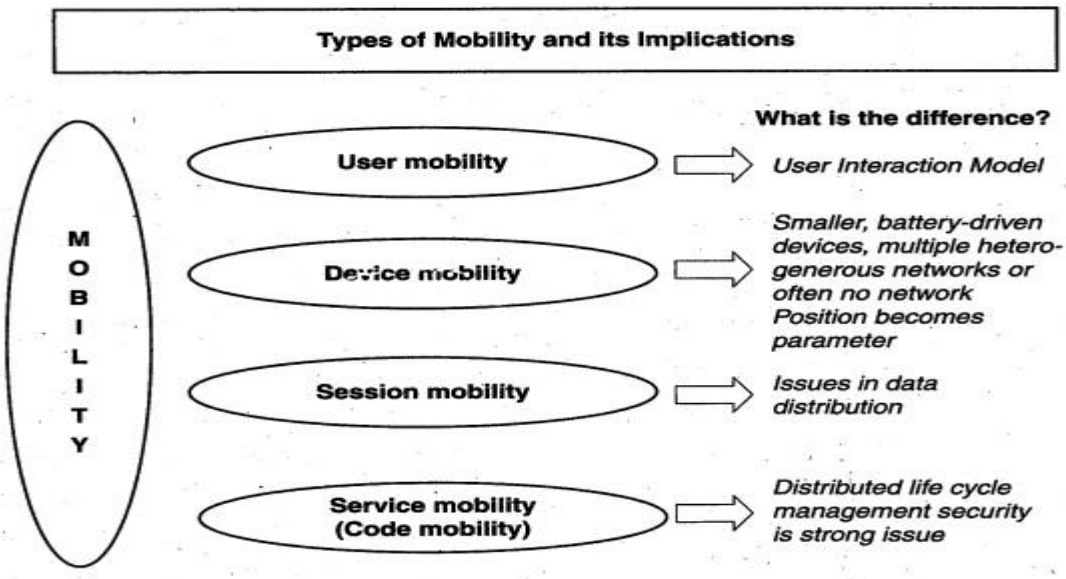

Figure: Mobility types and implications

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

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

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

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

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 mobile devices.
Some eminent kinds of attacks to which mobile devices are subjected to are: push attacks, pull attacks and crash attacks.
Authentication services security is important given the typical attacks on mobile devices through wireless networks: Dos attacks, traffic analysis, eavesdropping, man-in-the-middle attacks and session hijacking. Security measures in this scenario come from Wireless Application Protocols (WAPs), use of VPNs, media access control (MAC) address filtering and development in 802.xx standards.

Attacks on Mobile-Cell Phones:

- **Mobile Phone Theft:**

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

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

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

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

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

Organizational security Policies and Measures in Mobile Computing Era:
Proliferation of hand-held devices used makes the cybersecurity issue graver than what we would tend to think. People have grown so used to their hand-helds they are treating them like wallets! For example, people are storing more types of confidential information on mobile computing devices than their employers or they themselves know; they listen to musicusing their-hand-held devices.One should think about not to keep credit card and bank

account numbers, passwords, confidential E-Mails and strategic information about organization, merger or takeover plans and also other valuable information that could impact stock values in the mobile devices. Imagine the business impact if an employee's USB, pluggable drive or laptop was lost or stolen, revealing sensitive customer data such as credit reports, social security numbers (SSNs) and contact information.

Operating Guidelines for Implementing Mobile Device Security Policies

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

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

Organizational Policies for the Use of Mobile Hand-Held Devices

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

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