DON BOSCO INSTITUTE OF TECHNOLOGY, MUMBAI - 400 070
Department of Computer Engg. & Info. Technology
(Academic Year ODD Semester 2021 – 2022)

Course Code and Name : ILO 7016 - Cyber Security and Laws (BE Sem VII)

NAME:Hayden Cordeiro **BECOMPS** **ROLL NO.: 05**

ASSIGNMENT 1

Q1. What is Cybercrime? Who are Cybercriminals? Explain?

- Cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime is carried out by individuals or organizations. Cybercrime aims to damage computers for reasons other than profit. These could be political or personal.
- Cybercriminals are individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data, and generating profit.
- Cybercriminals are known to access the cybercriminal underground markets found in the deep web to trade malicious goods and services, such as hacking tools and stolen data. Cybercriminal underground markets are known to specialize in certain products or services.

Q2. Classify Cybercrimes? Explain with examples?

Crime against the Individuals: Crimes that are committed by the cyber criminals against an individual or a person. A few cyber crimes against individuals are:

- Harassment via electronic mails.
- Dissemination of obscene material.
- Cyber-stalking.
- Defamation.
- Indecent exposure.
- Cheating.
- Unauthorized control/access over computer systems.
- Email spoofing.
- Fraud.

Crimes against Property: These types of crimes include vandalism of computers, Intellectual (Copyright, patented, trademark etc) Property Crimes, Online threatening etc. Intellectual property crime includes:

- Computer vandalism.
- Transmitting virus.
- Net-trespass.
- Unauthorized access / control over computer systems.
- Internet thefts.
- Intellectual Property crimes- Software piracy, Copyright infringement, Trademark infringement.

Crime against Organization: Crimes done to threaten the international governments or any organization by using internet facilities. These cyber crimes are known as cybercrimes against Organization. These crimes are committed to spread terror among people. Cyber terrorism is referred as crimes against a government. Cybercrimes against Government includes cyber attack on the government website, military website or cyber terrorism etc.

- Unauthorized access / control over computer systems.
- Cyber terrorism against the government organization.
- Possession of unauthorized information.
- Distribution of Pirate software.

Crime against Society: Those cybercrimes which affects the society interest at large are known as cyber crimes against society, which include:

- Child pornography.
- Indecent exposure of polluting the youth financial crimes.
- Sale of illegal articles.
- Trafficking.
- Forgery.

- Online gambling.

Q3. Explain about legal perspectives of Cybercrimes?
Advances in information and communications technologies have revolutionised government scientific , educational and commercial infrastructures. The IT infrastructure has become an integral part of the critical infrastructure which supports national capabilities such as power grids, emergency communication systems, financial systems , defence systems and air traffic control networks. The operational stability and security of critical information infrastructure is vital for economic security of the country.

Q4. Explain about Indian perspectives of Cybercrimes?
Cyber crime is a crime done with the misuse of information technology for unauthorized or illegal access, electronic fraud; like deletion, alteration, interception, concealment of data, forgery etc.. Cyber crime is an international crime as it has been affected by the global revolution in information and communication technologies (ICTs). It has affected the global community. To combat cyber crime, India enacted the Information Technology Act,2000 which was drastically amended in the year 2008 providing more powerful and stringent law.
Cyber crime in India resulted in 29.9 million people being victim of cybercrime involving direct financial losses to the tune of $4 billion and $3.6 billion in terms of time spent in resolving the crime.
4 out of 5 online adults(80%) being victim of cyber crime

Q5. Discuss about Cybercrime and the Indian ITA 2000?
Cyber crime can be defined as :- a crime done through a computer, an illegal activity committed on the internet, where the computer acts as a tool for crime, and exposed to internet security.
The Information Technology (IT) Act 2000 can be defined as :- an act passed by the Indian Parliament, contains cyber laws, provides legal framework, safeguards e-commerce and e-data interchange.
Some of the objectives of the IT Act 2000 are as follows :-
- To facilitate maintenance of electronic records.
- To facilitate legality to electronic transactions.
- To facilitate electronic filing.
- To amend various other acts.

Features of the Information Technology Act, 2000
- All electronic contracts made through secure electronic channels are legally valid.
- Legal recognition for digital signatures.
- Security measures for electronic records and also digital signatures are in place
- A procedure for the appointment of adjudicating officers for holding inquiries under the Act is finalized
- Provision for establishing a Cyber Regulatory Appellant Tribunal under the Act.
- Further, this tribunal will handle all appeals made against the order of the
- Controller or Adjudicating Officer.
- An appeal against the order of the Cyber Appellant Tribunal is possible only in the High Court

Q6. How the Criminals Plan the Attacks? Explain with examples?
Cyber Criminals use many tools and methods to locate the vulnerability of their victim.
Attackers can be categorized as inside attacker or outside attacker. Attacks performed within the organization are called inside attacks whereas attackers getting information from outside is called outside attack. Inside attacks are always more dangerous than outside, because inside attackers have more resources than outsiders.
- Passive Attacks: Passive attacks used to gain information about an individual or organization. It exploits confidential information. Passive attacks involve gaining data about a target without target knowledge.
- Active attacks: Active attack mostly used to manipulate or alter the system. It may affect the integrity, authenticity and availability of data. Information from the passive phase acts as input to the active phase. In this phase attackers verify and gather information (IP address, network range, hidden server, personal information). This is very important from a cyber attacker point of view, it provides security measures.

Q7. What are Cyber Offenses? Discuss?

Cyber offences are the illegitimate actions, which are carried out in a classy manner where either the computer is the tool or target or both

The offences included in the I.T. Act 2000 are as follows –

- Tampering with the computer source documents.
- Hacking with a computer system.
- Publishing of information which is obscene in electronic form.
- Power of Controller to give directions.
- Directions of Controller to a subscriber to extend facilities to decrypt information.
- Protected system.
- Penalty for misrepresentation.
- Penalty for breach of confidentiality and privacy.
- Penalty for publishing Digital Signature Certificate false in certain particulars.
- Publication for fraudulent purposes.
- Act to apply for offence or contravention committed outside India Confiscation.
- Penalties or confiscation not to interfere with other punishments.
- Power to investigate offences.

Q8. Write about Cyber café and Cybercrimes?

Cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime is carried out by individuals or organizations. Cybercrime aims to damage computers for reasons other than profit. These could be political or personal.

A cybercafe is a type of business where computers are provided for accessing the internet, playing games, chatting with friends or doing other computer-related tasks. In most cases, access to the computer and internet is charged based on time. There are many internet cafes located worldwide, and in some countries they are considered the primary form of internet access for people. Cybercriminals prefer cybercafes to carry out their activities. The criminals tend to identify one particular personal computer PC to prepare it for their use. Cybercriminals will visit these cafes at a particular time and on the prescribed frequency, maybe alternate day or twice a week.

Q9. What is Proliferation of Mobile and Wireless Devices? Explain?

Across the globe, the usage of small wireless mobile devices such as PDAs, Blackberrys and smartphones is growing faster than the Internet. The number of smartphones worldwide crossed 130 million by the end of 2008, according to IDC. As wireless devices grow in sophistication and numbers, it’s no surprise that virus writers, hackers, and organized criminals have begun targeting them.It’s surprising is how quickly they’ve found so many ways to exploit them. Enterprises should not underestimate this emerging threat. The proliferation of mobile phones will continue as mobile data traffic jumps. 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 the 1990s. They are as follows:

1. **Portable computer:** It is a general-purpose computer that can be easily moved from one place to another, but cannot be used while in transit, usually because it requires some "setting-up" and an AC power source.
2. **Tablet PC:** It lacks a keyboard, is shaped like a slate or a paper notebook and has features of a touchscreen with a stylus and handwriting recognition software. Tablets may not be best suited for applications requiring a physical keyboard for typing, but are otherwise capable of carrying out most tasks that an ordinary laptop would be able to perform.
3. **Internet tablet:** It is an Internet appliance in tablet form. Unlike a Tablet PC, the Internet tablet does not have much computing power and its applications suite is limited. Also it cannot replace a general-purpose computer. The Internet tablets typically feature an MP3 and video player, a Web browser, a chat application and a picture viewer.
4. **Personal digital assistant (PDA):** It is a small, usually pocket-sized, computer with limited functionality. It is intended to supplement and synchronize with a desktop computer, giving access to contacts, address book, notes, E-Mail and other features.
5. **Ultra Mobile (PC):** It is a full-featured, PDA-sized computer running a general-purpose operating system (OS).
6. **Smartphone:** It is a PDA with an integrated cell phone functionality. Current Smartphones have a wide range of features and installable applications.
7. **Carputer:** It is a computing device installed in an automobile. It operates as a wireless computer,

sound system, global positioning system (GPS) and DVD player. It also contains word processing software and is Bluetooth compatible.

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

Q10.Discuss about the Cybercrime activities in Mobile Devices?

- **Data Leakage:** Mobile apps are often the cause of unintentional data leakage.For example, "riskware" apps pose a real problem for mobile users who grant them broad permissions, but don't always check security. These are typically free apps found in official app stores that perform as advertised, but also send personal—and potentially corporate—data to a remote server, where it is mined by advertisers, and sometimes, by cybercriminals.
- **Unsecured Wi-Fi:** To be safe, use free Wi-Fi sparingly on your mobile device. And never use it to access confidential or personal services, like banking or credit card information.
- Network Spoofing: Network spoofing is when hackers set up fake access points—connections that look like Wi-Fi networks, but are actually traps—in high-traffic public locations such as coffee shops, libraries and airports.
- **Phishing Attacks:** Mobile device users are also more susceptible because email apps display less information to accommodate the smaller screen sizes..Even when opened, an email may only display the sender's name unless you expand the header information bar. Never click on unfamiliar email links.
- **Spyware:** In many cases, it's not malware from unknown attackers that users should be worried about, but rather spyware installed by spouses, coworkers or employers to keep track of their whereabouts and activity.

Q11. Explain about Credit card frauds in the Mobile and Wireless Computing era?

Cybercrime that is 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. Mobile credit card transactions are now very common; new technologies combine low-cost mobile phone technologies with the capabilities of a point-of-sale (POS) terminal. Wireless credit card processing is a very desirable system, because it allows businesses to process transactions from mobile locations quickly, efficiently and professionally. Skimming to Commit Fraud is a kind of crime in which dishonest employees make unlawful copies of credit or debit cards with the help of a 'skimmer'. A skimmer is a gadget that captures credit card numbers and other account information which should be personal. The data and records held on either the magnetic stripe on the lower back of the deposit card or the records saved on the smart chip are copied from one card to another.

Q12. What are different security challenges posed by mobile devices? Explain?

Mobile phone security threats generally include application based, web-based, network-based and physical threats.

1. Application based threat:

Most applications are downloadable and pose the most common risk for mobile users; most devices don't do much on their own, and it is the applications that make them so awesome and we all download apps. If it comes to apps the risks run from bugs and basic security risks on the low end of the scale all the way through malicious apps with no other purpose to commit cyber crime.

Malware,Spyware, Privacy, Zero Day Vulnerabilities

2. Web based threat:

According to the nature of mobile use, the fact that we have our devices with us everywhere we go and are connecting to the Internet while doing so, they face a number of unique web-based threats as well as the run-of-the-mill threats of general Internet use.

Phishing Scams, Social Engineering, Drive By Downloads, Operating System Flaws

3. Network-based threat:

Any mobile devices which typically support a minimum of three network capabilities making them three-times vulnerable to network-based attack. And a network often found on a mobile includes cellular, WiFi and Bluetooth.

Network exploits, WiFi sniffing, Cross-Platform Attacks, BOYD

4. Physical Threats:

It happens any time, unlike a desktop sitting at your workstation, or even a laptop in your bag, a mobile device is subject to a number of everyday physical threats.

Loss/Theft: Loss or theft is the most unwanted physical threat to the security of your mobile device. Any device itself has value and can be sold on the secondary market after all your information is stolen and sold.

Q13. Discuss about Authentication Service Security?

There are two components of security in mobile computing: security of devices and security in networks. A secure network access involves authentication between the device and the base stations or Web servers. This is to ensure that only authenticated devices can be connected to the network for obtaining the requested services. No Malicious Code can impersonate the service provider to trick the device into doing something it does not mean to. Thus, the networks also play a crucial role in security of mobile devices.

Some eminent kinds of attacks to which mobile devices are subjected 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.x standards.

Q14. Write about Mobile/Cell Phone attacks?

- **SMiShing:** SMiShing has become common now as smartphones are widely used. SMiShing uses Short Message Service (SMS) to send fraud text messages or links. The criminals cheat the user by calling. Victims may provide sensitive information such as credit card information, account information, etc. Accessing a website might result in the user unknowingly downloading malware that infects the device.
- **War driving:** War driving is a way used by attackers to find access points wherever they can be. With the availability of free Wi-Fi connection, they can drive around and obtain a very huge amount of information over a very short period of time.
- **WEP attack:** Wired Equivalent Privacy (WEP) is a security protocol that attempts to provide a wireless local area network with the same level of security as a wired LAN. Since physical security steps help to protect a wired LAN, WEP attempts to provide similar protection for data transmitted over WLAN with encryption.
- **WPA attack:** Wi-Fi Protected Access (WPA) and then WPA2 came out as improved protocols to replace WEP. WPA2 does not have the same encryption problems because an attacker cannot recover the key by noticing traffic. WPA2 is susceptible to attack because cyber criminals can analyze the packets going between the access point and an authorized user.
- **Bluejacking:** Bluejacking is used for sending unauthorized messages to another Bluetooth device. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers and other devices.
- **Replay attacks:** In Replay attack an attacker spies on information being sent between a sender and a receiver. Once the attacker has spied on the information, he or she can intercept it and retransmit it again thus leading to some delay in data transmission. It is also known as playback attack.
- **Bluesnarfing:** It occurs when the attacker copies the victim's information from his device. An attacker can access information such as the user's calendar, contact list, e-mail and text messages without leaving any evidence of the attack.
- **RF Jamming:** Wireless signals are susceptible to electromagnetic interference and radio-frequency interference. Radio frequency (RF) jamming distorts the transmission of a satellite station so that the signal does not reach the receiving station

Q15. Discuss about the Security implications for Organizations?

- Most organizations fail to see the long-term significance of keeping track of who owns what kind of mobile devices. Mobile devices of employees should be registered in the corporate asset register irrespective of whether or not the devices have been provided by the organization. In addition, close monitoring of these devices is required in terms of their usage. When an employee leaves, it is important to remove his/her logical as well as physical access to corporate resources because employees (for malicious or other reasons) could be using their mobile devices to connect into the corporate networks. Thus, mobile devices that belong to the company should be returned to the IT department and, at the very least, should be deactivated and cleansed.
- Organization has to have a policy in place to block ports while issuing the asset to the employee. However, sometimes the standard access controls with Windows OS do not allow the assignment of permissions for USB ports and restricting these devices becomes next to impossible. Disgruntled employees can connect a USB/small digital camera/MP3 player to the USB port of any unattended

computer and will be able to download confidential data or upload harmful viruses. As the malicious attack is launched from within the organization, firewalls and antivirus software are not alerted.

Q16. What are different Organizational measures for handling Mobile?

- **Mobile Devices Need Antimalware Software:** Anybody who wants to use a mobile device to access the Internet should install and update antimalware software for his or her smartphone or tablet. This goes double for anyone who wants to use such a device for work.
- **Secure Mobile Communications:** Most experts recommend that all mobile device communications be encrypted as a matter of course, simply because wireless communications are so easy to intercept and snoop on. Those same experts go one step further to recommend that any communications between a mobile device and a company or cloud-based system or service require use of a VPN for access to be allowed to occur.
- **Require Strong Authentication, Use Password Controls:** Many modern mobile devices include local security options such as built-in biometrics — fingerprint scanners, facial recognition, voiceprint recognition and so forth — but even older devices will work with small, portable security tokens.Companies or organizations should consider whether the danger of loss and exposure means that some number of failed login attempts should cause the device to wipe its internal storage clean.
- **Control Third-party Software:** Companies or organizations that issue mobile devices to employees should establish policies to limit or block the use of third-party software. This is the best way to prevent possible compromise and security breaches.
- **Create Separate, Secured Mobile Gateways:** Directing mobile traffic through special gateways with customized firewalls and security controls in place — such as protocol and content filtering and data loss prevention tools — keeps mobile workers focused on what they can and should be doing away from the office. This also adds protection to other, more valuable assets they don't need to access on a mobile device anyway.
- **Choose Secure Mobile Devices, Help Users Lock Them Down:** Mobile devices should be configured to avoid unsecured wireless networks, and Bluetooth should be hidden from discovery. In fact, when not in active use for headsets and headphones, Bluetooth should be disabled altogether.
- **Perform Regular Mobile Security Audits, Penetration Testing:** At least once a year, companies and organizations should hire a reputable security testing firm to audit their mobile security and conduct penetration testing on the mobile devices they use.

Q17. What are different Security policies on Laptops and Wireless devices? Explain?

Physical security controls for laptops: Keep your laptop in your possession and within sight whenever possible.

Virus protection of laptops: Viruses are a major threat to and laptops are particularly vulnerable if their anti-virus software is not kept up-to-date. The anti-virus software MUST be updated at least monthly. Always virus-scan any files downloaded to your computer from any source.

Controls against unauthorized access to laptop data: You must use approved encryption software on all corporate laptops, choose a long, strong encryption password/phrase and keep it secure. If your laptop is lost or stolen, encryption provides extremely strong protection against unauthorized access to the data.

Unauthorized software: Do not download, install or use unauthorized software programs. Unauthorized software could introduce serious security vulnerabilities into the networks as well as affecting the working of your laptop.

Unlicensed software: Be careful about software licenses. Most software, unless it is specifically identified as “freeware” or “public domain software”, may only be installed and/or used if the appropriate license fee has been paid.

Backups: Unlike desktop PCs which are backed up automatically by IT, you must take your own backups of data on your laptop. The simplest way to do this is to login and upload data from the laptop to the network on a regular basis – ideally daily but weekly at least.