

Cyber Security - lecture 1

Contents

- ▶ Introduction to Cyber Crime
- ▶ Types of Cyber Crime
- ▶ Cyber Law
- ▶ Traditional Problems Associated with Cyber Crime [Computer Crime]
- ▶ Indian IT ACT 2000
- ▶ Indian IT ACT 2008

Introduction to Cyber Crime

- ▶ Cybercrime is the crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.
- ▶ Cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones.
- ▶ Cyber-crime is the latest and perhaps the most complicated problem in the cyber world.
- ▶ The enormous growth in electronic commerce (e-commerce) and online share trading has led to a sudden increase in incidents of cyber-crime.

Types of Cyber Crime

- ▶ Cybercrimes can be basically divided into following categories:
 - ▶ Cybercrimes against Individuals
 - ▶ Cybercrimes against Property
 - ▶ Cybercrimes against Government/Organizations
 - ▶ Cyber crimes against Society

Types of Cyber Crime - Contd.

- ▶ Cybercrimes against individuals
 - ▶ Harassment via electronic mails
 - ▶ Dissemination [publicize] of obscene material
 - ▶ Cyber-stalking - the repeated use of electronic communications to harass or frighten someone
 - ▶ Defamation - damaging the good reputation of someone
 - ▶ Indecent exposure.
 - ▶ Cheating.
 - ▶ Unauthorized control/access over computer system.
 - ▶ Email spoofing.

Types of Cyber Crime - Contd.

- ▶ Cybercrime against property. These crimes include:
 - ▶ Computer vandalism (destruction of others' property);
 - ▶ Transmission of harmful programs - Virus, malware etc.
 - ▶ Illegal transfer of funds from financial institutions;
 - ▶ Stealing secret information & data.
 - ▶ Unauthorized access / control over computer system
 - ▶ Intellectual Property crimes
 - ▶ Internet thefts : It is the use by an unauthorized person of the Internet hours paid for by another person.

Types of Cyber Crime - Contd.

- ▶ Cybercrime against Government/Organization
 - ▶ Unauthorized access / control over computer system.
 - ▶ Cyber terrorism against the government organization.
 - ▶ The medium of Cyberspace is used by individuals and groups to threaten the international governments as also to terrorize the citizens of a country.
 - ▶ This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website.
 - ▶ Distribution of Pirate software.

Types of Cyber Crime - Contd.

- ▶ Cybercrime against Society
 - ▶ Child pornography
 - ▶ Indecent exposure of polluting the youth financial crimes.
 - ▶ Sale of illegal articles.
 - ▶ Trafficking.
 - ▶ Forgery - [eg: Fake marksheets, Fake currency]
 - ▶ Online gambling

Cyber Law

- ▶ Cyber law is the part of the overall legal system that deals with the Internet, cyberspace, and their respective legal issues. Cyber law covers a fairly broad area, encompassing several subtopics including freedom of expression, access to and usage of the Internet, and online privacy. Generically, cyber law has been referred to as the Law of the Internet.
- ▶ Why are cyber laws needed?
 - ▶ Just like any law, a cyber law is created to help protect people and organizations on the Internet from malicious people on the Internet and help maintain order. If someone breaks a cyber law or rule, it allows another person or organization to take action against that person or have them sentenced to a punishment.

Traditional Problems Associated with Cyber Crime

- ▶ While criminals have always displayed an ability to adapt to changing technologies, law enforcement agencies and government institutions, bound by bureaucracy, have not.
- ▶ Computer crime, in particular, has proven a significant challenge to Law Experts personnel for a variety of reasons.
- ▶ Different challenges
 - ▶ Physicality and jurisdictional concerns
 - ▶ Lack of communication b/w agencies
 - ▶ Problems related with evidence
 - ▶ Inconsistency of law and community standards
 - ▶ Cost/benefit to criminal or hacker
 - ▶ Lack of Resources

Traditional Problems Associated with Cyber Crime - Contd.

- ▶ **Physicality and jurisdictional concerns**
 - ▶ Individuals sitting at their desk can enter various countries without the use of passports or documentation.
 - ▶ For successful prosecution it is necessary to get the specification of the crime scene i.e.,
 - ▶ Where did the crime actually occur?
 - ▶ Which laws apply?
 - ▶ Which agency is responsible for the investigation of a particular incident?
 - ▶ Which agency has primary jurisdiction over the thief?
- ▶ **Lack of communication b/w agencies**
 - ▶ lack of collaboration b/w agencies due to international concerns

Traditional Problems Associated with Cyber Crime - Contd.

- ▶ Inconsistency of law and community standards
 - ▶ definitions of obscenity, criminality, etc. - further complicated on the international level where some societies may tolerate or accept certain behaviors
- ▶ Problems related with evidence
 - ▶ Unsure about how to recognize evidence
 - ▶ Unsure about how to preserve evidence
- ▶ Cost/benefit to criminal or hacker
 - ▶ much less expensive and the risk of successful prosecution is less
 - ▶ do not need method of transportation
 - ▶ do not need funds
 - ▶ do not need storage capabilities
 - ▶ are not labor intensive and can be committed alone

Traditional Problems Associated with Cyber Crime - Contd.

- ▶ Lack of Resources
 - ▶ Traditional budget constraints
 - ▶ Nature of technology
 - ▶ Changes in the technology requires frequent training and updation.
 - ▶ By the time the old method may become obsolete
 - ▶ Cost of training
 - ▶ Extremely expensive training which is out of reach for many agencies.
 - ▶ Cost of additional personnel
 - ▶ For every officer transferred to technology crime, another must be recruited, hired, and trained to take his/her place.
 - ▶ Cost of hardware
 - ▶ equipment soon becomes obsolete, precluding the purchase of pricey components

Traditional Problems Associated with Cyber Crime - Contd.

- ▶ Lack of Resources
 - ▶ Cost of software
 - ▶ Forensic software is extremely expensive.
 - ▶ Cost of laboratory
 - ▶ Inability to compete with private industry
 - ▶ Individuals with forensic training are highly prized by corporations. Since they can afford to offer high salaries and lucrative benefit packages, they can successfully lure officers into private practice.

Indian IT ACT 2000

- ▶ The primary source of cyber law in India is the Information Technology Act, 2000 (IT Act).
- ▶ The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.
- ▶ Information Technology Act 2000 consisted of 94 sections segregated into 13 chapters.
- ▶ Cyber law of India includes laws relating to
 - ▶ Cyber Crimes
 - ▶ Electronic and Digital Signatures
 - ▶ Intellectual Property
 - ▶ Data Protection and Privacy

Indian IT ACT 2000 - Contd.

▶ Cyber-crime

- ▶ Cyber-crime is the latest and perhaps the most complicated problem in the cyber world.
- ▶ Cyber-crimes are unlawful acts where computer is used either as a tool; or a target; or both.
- ▶ The enormous growth in electronic commerce (e-commerce) and online share trading has led to a sudden increase in incidents of cyber-crime.

Indian IT ACT 2000 - Contd.

▶ Electronic Signature

- ▶ Electronic Signatures are used to authenticate electronic records. Digital Signatures are one type of electronic signatures.
- ▶ Digital Signatures satisfy three major legal requirements:
 - ▶ Signer authentication;
 - ▶ Message authentication;
 - ▶ Message integrity.
- ▶ The technology and efficiency of digital signatures makes them more trustworthy than hand written signatures.

Indian IT ACT 2000 - Contd.

▶ Intellectual Property

- ▶ Intellectual property refers to creations of the human mind. The features of intellectual property that relate to cyber space are covered by Cyber law.
- ▶ Features of Intellectual Property
 - ▶ Copyright law in relation to computer software, source code, websites, cell phone content etc.
 - ▶ Licensing in terms of software and source code.
 - ▶ Trademark law with relation to domain names, meta tags, mirroring, framing, linking etc.
 - ▶ Semiconductor law which relates to the protection of semiconductor integrated circuits design and layouts.
 - ▶ Patent law in relation to computer hardware and software.

Indian IT ACT 2000 - Contd.

▶ Data Protection & Privacy

- ▶ Data Protection and Privacy Laws aim to achieve a fair balance between the privacy rights of the individual and the interests of data controllers such as banks, hospitals, email service providers etc.
- ▶ These laws seek to address the challenges to privacy caused by collecting, storing and transmitting data using new technologies.

Indian IT ACT 2008

- ▶ IT Act 2008, is the new version of Information Technology Act 2000, has provided additional focus on Information Security.
- ▶ It has added several new sections on offences including Cyber Terrorism and Data Protection.
- ▶ The Information Technology Amendment Act, 2008 (IT Act 2008) has been passed by the parliament on 23rd December 2008 and came into force from October 27, 2009 onwards.