UNIT – IV

Cyber Law

Cyberspace

Cyberspace can be defined as an complicated environment that involves interactions between people, software, and services. It is maintained by the worldwide distribution of information and communication technology devices and networks.

With the benefits carried by the technological advancements, the cyberspace today has become a common pool used by citizens, businesses, critical information infrastructure, military and governments in a fashion that makes it hard to induce clear boundaries among these different groups. The cyberspace is anticipated to become even more complex in the upcoming years, with the increase in networks and devices connected to it.

Cybersecurity

Cybersecurity denotes the technologies and procedures intended to safeguard computers, networks, and data from unlawful admittance, weaknesses, and attacks transported through the Internet by cyber criminals.

Cyber crime

Globalization results in connecting people all around the world. The increasing access to and continuous use of technology has radically impacted the way in which people communicate and conduct their daily lives. The internet connects people and companies from opposite sides of the world fast, easily, and relatively economically. Nevertheless, the internet and computer can pose some threats which can have disparaging impact on civilisations. Cybercrime is a hazard against different organisations and people whose computers are connected to the internet.

Cybercrime is a dangerous crime involving computers or digital devices, in which a computer can be either a target of the crime, a tool of the crime or contain evidence of the crime. Cybercrime basically defined as any criminal activity that occurs over the Internet. There are many examples such as fraud, malware such as viruses, identity theft and cyber stalking. Earlier, cybercrime was committed mainly by individuals or small groups. Presently, it is observed that there is highly complex cybercriminal networks bring together individuals at global level in real time to commit crimes.

Today, criminals that indulge in cybercrimes are not motivated by ego or expertise. Instead, they want to use their knowledge to gain profits. They are using their capability to deceive and exploit people as they find it easy to generate money without having to do an honest work. Cybercrimes have become major threat today.

Classification of Cybercrimes:

1. Individual:

This type of cybercrime can be in the form of cyber stalking, distributing unwanted images, trafficking and "grooming". In present situation, law enforcement agencies are considering such cybercrime very serious and are joining forces worldwide to reach and arrest the committers.

2.Property:

Same as in the real world where a criminal can steal and pickpocket, even in the cyber world, offenders resort to stealing and robbing. In this case, they can steal a person's bank details and drain off money; misuse the credit card to make frequent purchases online; run a scam to get naive people to part with their hard earned money; use malicious software to gain access to an organization's website or disrupt the systems of the organization.

3.Government:

Crimes against a government are denoted to as cyber terrorism. If criminals are successful, it can cause devastation and panic amongst the citizen. In this class, criminals hack government websites, military websites or circulate propaganda. The committers can be terrorist outfits or unfriendly governments of other nations.

Need for Cyberlaw

There are various reasons why it is extremely difficult for conventional law to cope with cyberspace. Some of these are discussed below.

1. Cyberspace is an intangible dimension that is impossible to govern and regulate using conventional law.

2. Cyberspace has complete disrespect for jurisdictional boundaries . A person in India could break into a bank's electronic vault hosted on a computer in USA and transfer millions of Rupees to another bank in Switzerland, all within minutes. All he would need is a laptop computer and a cell phone.

3. Cyberspace handles gigantic traffic volumes every second. Billions of emails are crisscrossing the globe even as we read this, millions of websites are being accessed every minute and billions of dollars are electronically transferred around the world by banks every day.

4. Cyberspace is absolutely open to participation by all. A ten-year-old in Bhutan can have a live chat session with an eight-year-old in Bali without any regard for the distance or the anonymity between them.

5. Cyberspace offers enormous potential for anonymity to its members. Readily available encryption software and steganographic tools that seamlessly hide information within image and sound files ensure the confidentiality of information exchanged between cyber-citizens.

6. Cyberspace offers never-seen-before economic efficiency. Billions of dollars worth of software can be traded over the Internet without the need for any government licenses, shipping and handling charges and without paying any customs duty.

7. Electronic information has become the main object of cyber crime. It is characterized by extreme mobility, which exceeds by far the mobility of persons, goods or other services. International computer networks can transfer huge amounts of data around the globe in a matter of seconds.

8. A software source code worth crores of rupees or a movie can be pirated across the globe within hours of their release.

9. Theft of corporeal information (e.g. books, papers, CD ROMs, floppy disks) is easily covered by traditional penal provisions. However, the problem begins when electronic records are copied quickly, inconspicuously and often via telecommunication facilities. Here the "original" information, so to say, remains in the "possession" of the "owner" and yet information gets stolen.

Importance of Cyberlaw

Cyberlaw is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyberlaws is a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives.

Features of Cyber Laws

Setting up the rules, regulations, and specific details of cyber law is something that is fairly new and changing every day. The laws have had a hard time keeping up with all the various technologies and formats available for people. Even with the constant changes there are very specific rights that people and businesses still have. The cyber laws are designed to make sure that everybody is protected and that the Internet is not used as a tool to harm or hurt people or industry. Here are some of the basic fundamentals that these laws provide people and businesses

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

E- Contract

E-contract is any kind of contract formed in the course of e-commerce by the interaction of two or more individuals using electronic means, such as e-mail, the interaction of an individual with an electronic agent, such as a computer program, or the interaction of at least two electronic agents that are programmed to recognize the existence of a contract

Types of Cyber Crimes:

1. Unauthorized Access and Hacking:

In this category, a person's computer is broken into so that his personal or sensitive information can be accessed. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location. Many crackers also try to gain access to resources through the use of password cracking softwares. Hackers can also monitor what users do on their computer and can also import files on their computer. A hacker could install several programs on to their system without their knowledge. Such programs could also be used to steal personal information such as passwords and credit card information.

2.Theft:

This type of cybercrime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the FBI.

3.Cyber Stalking:

This is a type of online harassment wherein the victim is endangered to a barrage of online messages and emails. Normally, these stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk.

4.Identity Theft:

This is a major problem with people using the Internet for cash transactions and banking services. In this cybercrime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card, full name and other sensitive information to drain off money or to buy things online in the victim's name. The identity thief can use person's information to fraudulently apply for credit, file taxes, or get medical services. It can result in major financial losses for the victim and even spoil the victim's credit history.

5.Malicious Software:

This software, also called computer virus is Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to gather sensitive information or data or causing damage to software present in the system.

6.Software piracy:

It is a theft of software through the illegal copying of genuine programs. Distribution of products intended to pass for the original. If an individual with a single user license loads the software onto a friend's machine, or if a company loads a software package onto each employee's machine without buying a site license, then both the single user and the company have broken the terms of the software license agreement and are therefore guilty of software piracy. Software piracy involves the unauthorized use, duplication, distribution, or sale of commercially available software.

7. Denial of service Attack:

This is an attack in which the criminal floods the bandwidth of the victim’s network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide. This kind of attack is designed to bring the network to crash by flooding it with useless traffic.

8. Virus attacks:

Viruses are the programs that have the capability to infect other programs and make copies of itself and spread into other program. Programs that multiply like viruses but spread from computer to computer are called as worms. These are malicious software that attach themselves to other software. Virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious. Viruses usually affect the data on a computer, either by altering or deleting it. On the other hand worms merely make functional copies of themselves and do this repeatedly till they eat up all the available.

9.Logic Bombs

A logic bomb is a program that runs at a specific date and/or time to cause unwanted and/or unauthorized functions. It can effect software or data, and can cause serious damage to a system. For example, a disgruntled employee may write a program designed to crash the system one month after he plans to quit the company. When this date and time arrives, the program then executes. In other words, the bomb goes off.

10.Trojan Horse

In computer terms, Trojan Horses live up to the name derived from the Greek story. Covert instructions are hidden inside of a program. These instructions are embedded in software or email, and may provide any number of undesired or unauthorized functions. Once opened, they may modify or damage data, or send information over the Internet

11. Salami attacks :

These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month.

12. Phishing:

Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

13.Web Hijacking:

Web hijacking means taking forceful control of another person's website. In this case the owner of the website loses control over his website and its content.

14.Computer vandalism:

It is a type of cybercrime that Damages or destroys data rather than stealing. It transmits virus.

15.Cyber terrorism:

It is a use of Internet based attacks in terrorist activities. Technology savvy terrorists are using 512-bit encryption, which is impossible to decrypt.

16. Email spoofing :

Email spoofing refers to email that appears to originate from one source but actually has been sent from another source. Email spoofing can also cause monetary damage.

17. Cyber Defamation:

When a person publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends, it is termed as cyber defamation.

18. Forgery:

Computers, printers and scanners are used to forge counterfeit currency notes, postage and revenue stamps, mark sheets etc. These are made using computers, and high quality scanners and printers.

19. Email bombing :

Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.

20. Breach of Privacy and Confidentiality :

Confidentiality means non disclosure of information to unauthorized or unwanted persons. In addition to Personal information some other type of information which useful for business and leakage of such information to other persons may cause damage to business or person, such information should be protected.

21. Data diddling:

Data diddling involves changing data prior or during input into a computer. The information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. It also include automatic changing the financial information for some time before processing and then restoring original information.

22. E-commerce/ Investment Frauds:

An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online are never delivered. The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site. Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.

Problems of enforcement :

1.Jurisdiction

Jurisdiction is which agency has the authority to investigate and prosecute different types of crimes. There are several factors that determine who has jurisdiction over a case, like:

Which branch of the law. Cases can fall into a few different branches of the law, including criminal, civil, and regulatory law.

Type of case. The type of case is a determining factor. Each system employs different agencies responsible for different types of cases.

Severity of crime. The severity of the crime committed also plays a role. Different agencies and courts deal with different levels of severity.

Level of government. The last determining factor in jurisdiction has to do with which level of government the crime falls into, and some crimes fit into different laws at different levels of the government.

2.Location

Related to jurisdiction is the geographical location. A cyber criminal may be operating outside a law enforcement agencies jurisdiction, like in another state or even another country.

3.Anonymity

“Who done it?” is another factor making it difficult to enforce computer crime law. Finding out the identity of the criminal and where they are located can be very difficult. This is compounded by the fact that there are services available to mask IP address.

4.Evidence

In any crime scene investigation in the movies, a detective can carefully pluck evidence off a couch with a pair of tweezers, drop it into a bag, and examine it later. Physical evidence is easier to find and preserve than digital evidence. Digital evidence is fragile, and it can be hard to track down. A cyber criminal may commit theft through the servers of innocent users. Following the chain of evidence to the original server is difficult.

Effects of Cyber Crime

Criminals take advantage of technology in many different ways. The Internet, in particular, is a great tool for scammers and other miscreants, since it allows them to ply their trade while hiding behind a shield of digital anonymity. Cyber crime affects society in a number of different ways, both online and in the offline world.

1.Loss Of Revenue

One of the main effects of cyber crime on a company is a loss of revenue. This loss can be caused by an outside party who obtains sensitive financial information, using it to withdraw funds from an organization. It can also occur when a business's e-commerce site becomes compromised--while inoperable, valuable income is lost when consumers are unable to use the site.

2.Waste Of Time

Another major effect or consequence of cyber crime is the time that is wasted when IT personnel must devote great portions of their day handling such incidences. Rather than working on productive measures for an organization, many IT staff members spend a large percentage of their time handling security breaches and other problems associated with cyber crime.

3.Damaged Reputations

In cases where customer records are compromised by a security breach associated with cyber crime, a company's reputation can take a major hit. Customers whose credit cards or other financial data become intercepted by hackers or other infiltrators lose confidence in an organization and often begin taking their business elsewhere.

4.Reduced Productivity

Due to the measures that many companies must implement to counteract cyber crime, there is often a negative effect on employees' productivity. This is because, due to security measures, employees must enter more passwords and perform other time-consuming acts in order to do their jobs. Every second wasted performing these tasks is a second not spent working in a productive manner.

5.Identity Theft

Becoming the victim of cyber crime can have long-lasting effects on your life. One common technique scammers employ is phishing, sending false emails purporting to come from a bank or other financial institution requesting personal information. If you hand over this information, it can allow the criminal to access your bank and credit accounts, as well as open new accounts and destroy your credit rating. This type of damage can take months or even years to fix, so protecting your personal information online is an important skill to learn.

6.Security Costs

Cyber criminals also focus their attacks on businesses, both large and small. Hackers may attempt to take over company servers to steal information or use the machines for their own purposes, requiring companies to hire staff and update software to keep intruders out. According to EWeek, a survey of large companies found an average expenditure of $8.9 million per year on cyber security, with 100 percent of firms surveyed reporting at least one malware incident in the preceding 12 months and 71 percent reporting the hijacking of company computers by outsiders.

7.Monetary Losses

The overall monetary losses from cyber crime can be immense. According to a 2012 report by Symantec, more than 1.5 million people fall victim to some sort of cyber crime every day, ranging from simple password theft to extensive monetary swindles. With an average loss of $197 per victim, this adds up to more than $110 billion dollars lost to cyber crime worldwide every year. As consumers get wise to traditional avenues of attack, cyber criminals have developed new techniques involving mobile devices and social networks to keep their illicit gains flowing.

8.Piracy

The cyber crime of piracy has had major effects on the entertainment, music and software industries. Claims of damages are hard to estimate and even harder to verify, with estimates ranging widely from hundreds of millions to hundreds of billions of dollars per year. In response, copyright holders have lobbied for stricter laws against intellectual property theft, resulting in laws like the Digital Millennium Copyright Act. These laws allow copyright holders to target file sharers and sue them for large sums of money to counteract the financial damage of their activities online.

Nature of E-Contract

1.The parties do not, in most cases, meet physically.

2. There are no physical boundaries.

3. No handwritten signature and in most times, no hand writing is required.

4. Since there is no utmost security, risk factor is very high.

5. Jurisdictional issues are a major setback on e-contracts in case of breach.

6. There is no single authority to monitor the whole process especially in shrink wrap contracts.

7. Digital Signatures are used and electronic records are used as evidences in court n when need arises. 8. The three main methods of contracting electronically are e-mail, World Wide Web (www), and Cyber contracts

Formation of Online Contracts or Electronic Contracts

Like an ordinary contract, e-contracts consisting of an offer and acceptance are enforceable. The conduct of the parties, such as exchanging e-mails or acceptance of a condition or terms or by downloading can also imply a contract. A variety of procedures are available for forming electronic/online contracts:

Email: The parties may create a valid contract by exchanging e-mail communications. Offers or acceptances can be completely exchanged via e-mail, or combined with paper documents, faxes, and oral debates.

Website Forms: In many cases, an e-commerce website offers for sale goods or services that are ordered by customers, by filling in and submitting an on-screen order form. The seller will enter into a contract once the order has been accepted. The products and services can be delivered off-line physically. A contract would also be valid for the terms of use of a website once the user accepts the contract by clicking “I Agree.”

EULA: The End User License Agreements also form valid contracts in which end users click “I Accept” or “I Accept the Terms.”

Types of electronic contracts

Shrink Wrap Contracts: These contracts are packed with the products and the usage of the particular products is deemed as an acceptance of the terms and conditions of the Contract. The user always has the option of returning the software if the new terms are not to his liking for a full refund. These contracts are generally containing in the CD Rom or software, and using of the CD Rom is considered as an acceptance of such terms and conditions.

Click Wrap Contracts: A click wrap Contract is mostly found as a part of a software. These agreements are rigid in nature and there is no chance of negotiation in it. Because the user of such software has only two options, that is to agree and use that particular software or to disagree with terms and conditions and not to use that particular software.

Browse Wrap Contracts: A browse wrap agreements are generally found in a website or a downloadable product, these contracts are published on a particular webpage and user have to find these terms and conditions by browsing to that particular web page. Because generally these contracts are hidden.

Digital Signature

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications.

Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages. Signers can also use them to acknowledge informed consent.

In many countries, including the United States, digital signatures are considered legally binding in the same way as traditional handwritten document signatures.