INTRODUCTION

Cyber crime, or computer related crime, is 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 but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)". Cybercrime may threaten a person or a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, unwarranted mass-surveillance, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise. Debarati Halder and K. Jaishankar further define cybercrime from the perspective of gender and defined 'cybercrime against women' as "Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones". Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyber warfare.1 A report (The Hiscox Cyber Readiness Report 2017) estimates that the annual damage to the global economy is at $450 billion; however, a Microsoft report shows that such survey-based estimates are "hopelessly flawed" and exaggerate the true losses by orders of magnitude. In 2016, a study by Juniper Research estimated that the costs of cybercrime could be as high as 2.1 trillion by 2019.4

Definition Cyber Crime

Defining cyber crimes, as "acts that are punishable by the Information Technology Act" would be unsuitable as the Indian Penal Code also covers many cyber crimes, such as email spoofing and cyber defamation, sending threatening emails etc. A simple yet sturdy definition of cyber crime would be "unlawful acts wherein the computer is either a tool or a target or both". In generally the term cybercrime was analyzed into two categories and defined thus:

I. Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

II. Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

Categories of Cyber crime

A. Against Individual

The cyber crimes which are done to harm a particular individual come under this category. The crime against individual can be such as cyber stalking, trafficking, grooming and distributing pornography. These crimes are very serious and the government is taking steps to protect the victims and arrest the criminals.

B. Against Property

The cyber crime which is done to harm the property of an individual or of an organization come under this category. This type of crime involves stealing and robbing i.e. criminals can steal person’s bank details and transfer money to his account; criminals can misuse the credit card details of the person to purchase online; criminals can use special software to steal organization’s confidential data; malicious software can also damage the hardware and software of the organization.

C. Against Government

Crimes against government are known as cyber terrorism. Cyber attacks against government are not as common as other two categories. Criminals attack government websites, military websites which create chaos among civilians.

Types of Cyber Crimes

Cyber crimes can be of the following types-

a) Hacking- In this type of crime person’s computer is accessed by criminals without the knowledge of person from remote locations. Hacking is done to access the personal, confidential or sensitive information from person’s computer. Hacking can also be done to change the passwords of login accounts either of social networking sites or any other business transaction site and use the information against them.

b) Theft- When a person violates or breaks the copyrights of a particular website and download songs, games, movies and software is known as theft. There are many websites which allow downloading the data that is copied from other websites. It is known as pirated data as the quality of data is not up to the mark.

c) Identity theft- In this type of crime, criminals steal data about person’s bank account number, credit card number, debit card and other confidential data to transfer money to his account or buy things online by acting as the original person i.e. the criminal stalks the identity of person and thus it is known as identity theft. This theft can result in huge economical loss to the victim.

d) Defamation- In this attack, the criminal hacks the email account of a person and sends mails using abusive languages to known persons’ mail accounts so as to lower the dignity or fame of the person.

e) Malicious software- These are the programs or software that are used to access the system to steal confidential data of the organization or this software can be used to damage the hardware and software of the system.

f) Cyber Stalking- This is the type of attack where online messages and e-mails are bombarded on victim’s system. In cyber stalking, internet is used to harass an individual, group or organization by using defamations, identity theft, solicitation for sex, false accusations etc.


RESEARCH REVIEW International Journal of Multidisciplinary

© RRJM 2015, All Rights Reserved

36 | P a g e
1860 protect property rights. The Information Technology Act deals with the hacking, tampering with computer source documents, publishing of information, which is obscene in electronic form, child pornography and breach of confidentiality & privacy, while the cyber crime other than those mentioned under the IT Act include cyber stalking, cyber squatting, data diddling, cyber defamation, Trojan attack, forgery, financial crimes, internet time theft, virus/worm attack, E-mail spoofing, Email bombing, salami attack and web jacking.6

The IT Act, 2000 penalizes cyber contraventions (section 43-a to h) and cyber offences (sections 65 to 74). The former category includes gaining unauthorized access and downloading or extracting data stored in computer systems or networks. Such actions may result in civil prosecution. The latter category covers serious offences like tampering with computer source code, hacking with intent to cause changes and breach of confidentiality and privacy.

**POSITIVE ASPECTS OF THE IT ACT, 2000**

a) Prior to the enactment of the IT Act, 2000 even an e-mail was not accepted under the prevailing statutes of India as an accepted legal form of communication and as evidence in a court of law. But the IT Act, 2000 changed this scenario by legal recognition of the electronic format. Indeed, the IT Act, 2000 is a step forward.

b) From the perspective of the corporate sector, companies shall be able to carry out electronic commerce using the legal infrastructure provided by the IT Act, 2000. Till the coming into effect of the Indian Cyber law, the growth of electronic commerce was impeded in our country basically because there was no legal infrastructure to regulate commercial transactions online.

c) Corporate will now be able to use digital signatures to carry out their transactions online. These digital signatures have been given legal validity and sanction under the IT Act, 2000.

d) In today’s scenario, information is stored by the companies on their respective computer system, apart from maintaining a back up. Under the IT Act, 2000, it shall now be possible for corporate to have a statutory remedy if any one breaks into their computer systems or networks and causes damages or copies data. The remedy provided by the IT Act, 2000 is in the form of monetary damages, by the way of compensation, not exceeding Rs. 1, 00, 00,000.

e) IT Act, 2000 has defined various cyber crimes which includes hacking and damage to the computer code. Prior to the coming into effect of the Indian Cyber law, the corporate were helpless as there was no legal redress for such issues. But the IT Act, 2000 changes the scene altogether.


**NEGATIVE ASPECTS OF THE IT ACT, 2000**

a) The IT Act, 2000 is likely to cause a conflict of jurisdiction.

b) Electronic commerce is based on the system of domain names. The IT Act, 2000 does not even touch the issues relating to domain names. Even domain names have not been defined and the rights and liabilities of domain name owners do not find any mention in the law.

c) The IT Act, 2000 does not deal with any issues concerning the protection of Intellectual Property Rights I the context of the online environment. Contentious yet very important issues concerning online copyrights, trademarks and patents have been left untouched by the law, thereby leaving many loopholes.

d) As the cyber law is growing, so are the new forms and manifestations of cyber crimes. The offences defined in the IT Act, 2000 are by no means exhaustive. However, the drafting of the relevant provisions of the IT Act, 2000 makes it appear as if the offences detailed therein are the only cyber offences possible and existing. The IT Act, 2000 does not cove various kinds of cyber crimes and Internet related crimes. These Include:-

   a. Theft of Internet hours
   b. Cyber theft
   c. Cyber stalking
   d. Cyber harassment
   e. Cyber defamation
   f. Cyber fraud
   g. Misuse of credit card numbers
   h. Chat room abuse

e) The IT Act, 2000 has not tackled several vital issues pertaining to e-commerce sphere like privacy and content regulation to name a few. Privacy issues have not been touched at all.

f) Another grey area of the IT Act is that the same does not touch upon any anti-trust issues.

g) The most serious concern about the Indian Cyber law relates to its implementation. The IT Act, 2000 does not lay down parameters for its implementation. Also, when internet penetration in India is extremely low and government and police officials, in general are not very computer savvy, the new Indian cyber law raises more questions than it answers. It seems that the Parliament would be required to amend the IT Act, 2000 to remove the grey areas mentioned above.

**CYBER SECURITY**

A branch of technology basically known as cyber security or information security applied to networks and computers, the objective carries protection of data or information and the property from the thefts, natural disaster, or corruption, and allowing the property and information to remain productive and accessible to its users. The Cyber security implies to the processes and the technologies which are designed to protect networks, computers and the data from the unauthorized
access, attacks, and vulnerabilities delivered via the Internet by cyber criminals.

PREVENTION TIPS FOR CYBER CRIME

a. Selecting a password that cannot be easily guessed: is the first step toward keeping passwords secure and away from the wrong hands. Strong passwords have eight characters or more and use a combination of letters, numbers and symbols (e.g., # $ % ! ?). Avoid using any of the following as your password: your login name, anything based on your personal information such as your last name, and words that can be found in the dictionary. Try to select especially strong, unique passwords for protecting activities like online banking.

b. Keep your passwords in a safe place: and try not to use the same password for every service you use online.

c. Change passwords on a regular basis: at least every 90 days. This can limit the damage caused by someone who has already gained access to your account. If you notice something suspicious with one of your online accounts, one of the first steps you can take is to change your password.

d. Protect your computer with security software: Several types of security software are necessary for basic online security. Security software essentials include firewall and antivirus programs. A firewall is usually your computer’s first line of defense—it controls who and what can communicate with your computer online. You could think of a firewall as a sort of “policeman” that watches all the data attempting to flow in and out of your computer on the Internet, allowing communications that it knows are safe and blocking “bad” traffic such as attacks from ever reaching your computer. The next line of defense many times is your antivirus software, which monitors all online activities such as email messages and Web browsing and protects an individual from viruses, worms, Trojan horse and other types malicious programs.

e. Protect your personal information Exercise caution: when sharing personal information such as your name, home address, phone number, and email address online. To take advantage of many online services, you will inevitably have to provide personal information in order to handle billing and shipping of purchased goods. Since not divulging any personal information is rarely possible, the following list contains some advice for how to share personal information safely online.

f. Keep an eye out for phony email messages: Things that indicate a message may be fraudulent are misspellings, poor grammar, odd phrasings, Web site addresses with strange extensions, Web site addresses that are entirely numbers where there are normally words, and anything else out of the ordinary. Additionally, phishing messages will often tell you that you have to act quickly to keep your account open, update your security, or urge you to provide information immediately or else something bad will happen. Don’t take the bait.

g. Don’t respond to email messages that ask for personal information: Legitimate companies will not use email messages to ask for your personal information. When in doubt, contact the company by phone or by typing in the company Web address into your Web browser. Don’t click on the links in these messages as they make take you to fraudulent, malicious Web sites.

h. Pay attention to privacy policies: on Web sites and in software. It is important to understand how an organization might collect and use your personal information before you share it with them.

i. Guard your email address: Spammers and phishers sometimes send millions of messages to email addresses that may or may not exist in hopes of finding a potential victim. Responding to these messages or even downloading images ensures you will be added to their lists for more of the same messages in the future. Also be careful when posting your email address online in newsgroups, blogs or online communities.

j. Review bank and credit card statements regularly: The impact of identity theft and online crimes can be greatly reduced if user can catch it shortly after their data is stolen or when user gets symptoms. Regularly check bank and credit card’s statements. Now, many banks and services use fraud prevention systems that call out unusual purchasing behavior.

CONCLUSION

In this modern era of technology, the role and usage of internet is increasing worldwide rapidly, therefore it becomes easy for cyber criminals to access any data and information with the help of their knowledge and their expertise. Cyber crime is an unlawful act or a menace that needs to be tackled firmly and effectively. Hacking is the method in which the criminals get access to the victim’s system without their knowledge. Cyber crime can be done mainly by using the technique of hacking. All the persons who use internet and especially those make money transactions through internet must be beware of the cyber criminals. It is the need of today’s world to have knowledge about the crimes that are associated with the internet. It is the duty of each one of us to be aware of the basic internet security like changing the passwords regularly, keeping long passwords, avoids disclosing personal information to strangers on the internet or entering credit card details on unsecured websites to avoid any fraud, etc. Government is also making efforts to have a control on these cyber crimes. Government has made cyber laws to help people learn about the cyber crimes and cyber security. New amendment should be including to the IT Act, 2000 to make it efficient and active against the crimes. The training and public awareness programs should be organized in the Companies as well as in common sectors. The number of the cyber cops in India should be increased. The jurisdiction problem is there in the implementation part which should be removed. Both the
government and people should work hand in hand to catch the criminals. Today in the present era there is a need to evolve a 'cyber-jurisprudence' based on which 'cyber-ethics' can be evaluated and criticized. Further there is a dire need for evolving a code of Ethics on the Cyber-Space and discipline. People who have been the victim of cyber crime should come forward and file a complaint against the crime in special anti cyber crime cells. Government should also employee officers with very high intelligent quotient and the knowledge about all the cyber crimes. This will help to catch the criminals very easily and all the criminals must be given hard punishments which can a lesson for millions of other cyber criminals. Awareness of the persons using internet will definitely help to curb the cyber crimes and once, all the people are aware of the cyber crime, no criminal would ever think to commit the cyber crime.