A Survey: Indian Cyber Law and Crime And It's Prevention Techniques

Sangeeta Singh - Assistant Professor, Department of Computer Science and Application, Madhav University Pindwara, Sirohi, Rajasthan, India
Email : sangeeta4u.singh@gmail.com

Abstract: Cyber law is used to represent the issue related to use of communication technology, mainly internet. In spite of that, now it is a crucial challenge to us because crime is gradually increases. This paper introduces some approach to prevent the various cybercrimes. India may succeed in fighting the problem of cybercrimes by adopting a synergetic approach where in technological measures. The purpose of this paper is Understanding Cyber law , Phenomena, challenge and Legal Response is to help each person in understanding the legal aspects of cyber law. It's aims to help better understand the national implication of growing cyber threats, to assess the requirements of existing national and to assist in establishing a legal foundation. So we discuss some of the legal and ethical issues. It creates systems to provide support for ethics in order to avoid harm to the society.

Key Words: Cyber Laws, Cyber Crimes, Cyber victimization, I.T. Act.

INTRODUCTION:

The `Cyber Law' deals with the Computers and the Internet Rather we can say as a computerized process. The Information Technology Act, 2000 was introduced on 9th June, 2000. The Information Technology Act, 2000 came into force on 17th October, 2000. This Act was amended vide Notification dated 27th October, 2009. cyber law provides legal recognition to electronic documents and a framework to support e-filing and e-commerce transactions and also provides a legal framework to check cyber-crimes. Indian cyber law's are used to protected several illegal activities in cyber place. It encapsulates the legal issues related to use of the Internet. Computers are used by all the students, professionals, teachers, universities, and banks, supermarkets, in the entertainment field, in medical profession and also in higher education for advancement purpose.

Cyber Law is the law governing cyber space. " Cyber space " is a very wide term and includes computers , data storage devices, the Internet, networks, software, websites, emails and even electronic devices such as cell phones, ATM machines etc. Cyberspace also creates the illusion for people that most things are available cheaper or free, and all actions undertaken are acceptable everywhere. Sitting in front of a computer, a person accessing the internet is virtually relocated to a "generalized elsewhere" of distant places While the person inhabits this generalized everywhere, they may be Cyber Law.

"Cyber Security" means computer resource, communication devices, protecting information, equipment's, and information stored there in from illegal access, use, disclosure, disruption, alteration or destruction.
The word "cyber law" encompasses all the cases, statutes and constitutional provisions that affect persons and institutions who control the entry to cyber space and enable the people to access cyberspace or use their own devices to go "online".

(i) CYBER LAW INCLUDES LAWS RELATING TO:

- Justice Dispensation Systems For Cyber Crimes.
- Digital Signature And Electronic Signature
- Legal Recognition Of Electronic Documents
- Intellectual Property
- Offenses And Contraventions
- Data Protection And Privacy
- Central Government to notify Examiner of Electronic Evidence

(ii) NEED FOR CYBER LAW

There are various reasons why it is extremely difficult for conventional law to deal with cyberspace. Some of these are as follows:

- Cyberspace has complete disrespect for jurisdictional boundaries.

- Cyberspace handles gigantic traffic volumes every second. Millions of websites are being accessed every minute and billions of dollars are electronically transferred around the world by banks every day.
- Cyberspace is absolutely open to participation by all.
- Cyberspace is an impossible to govern and regulate using conventional law.
- 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.
- A software source code worth crores of rupees or a movie can be pirated across the globe within hours of their release.
- Theft of corporeal information is easily covered by traditional penal provisions.
- However, the problem begins when electronic records are copied quickly, unnoticeably and often via telecommunication facilities. Here the "original" information, so to say, remains in the "ownership" of the "owner" and yet information gets stolen.

(iii) SOME OF THE MAJOR TYPES OF CHALLENGES

- Computer fraud,
- Forgery of prohibitive data,
- Alteration of data,
- False entry in an authentic deed
- False entry in permit licence or passport
- Committing mischief with data.
- Data spying,
- Electronic record made wrongfully by public servant
- Unauthorized access of computer of a Govt. Deptt. Or agency

1. CYBER CRIMES:

"Cyber crime" is illegal acts . which is completed with the help of computer. Cyber-crimes can involve criminal activities such as mischief , theft, fraud, forgery and offense all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a new range of crimes that are addressed by the Information Technology Act, 2000. Indian Cyber Laws were official born on 17th October 2000 with the Information Technology Act. The ingenuity of cyber criminals is becoming clear when we look at the clever ways in which online frauds are being perpetrated. cyber criminals combines elements of fake, falsification and lost trust to obtain sensitive personal data like credit card details, PIN numbers, passwords, etc. of victims. The attackers then cheat the victims by using such personal information. Other forms of cyber-crimes include illegal access to data , hacking, alteration of information and E-mail based offences.

The Information Technology Act deals with the following cyber-crimes along with others:

(i) Tampering with computer Source Documents*:* A person who intentionally keeps secret, destroys the information , alters the data or causes another to conceal, destroys the information , alters the data any computer source code used for a computer. When the computer source code is required to be kept or maintained by law is punishable. For instance, hiding the C.D.ROM in which the source code files are stored, making a C File into a CPP File or removing the read only attributes of a file.

(ii) Hacking*:* Hacking is usually unauthorized access of a computer system and network. Hackers usually - hack on a problem until they find a solution, and keep trying to make their equipment work in new and more efficient ways. A hacker can be a Code Hacker, Cracker or a Cyber Punk. Whoever with the goal to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value.

(iii) Publishing of Information: A person who publishes or causes to be published in the electronic form, any material which is lascivious, or if its cause is such as to tend to deprave and corrupt persons who are likely to read, see or hear the matter contained or embodied in it, is liable to punishment. The important ingredients of such an offence are publishing or transmitting or causing to be published (to produced the effect of publishing), pornographic material in the electronic form.

(iv) Child Pornography:. The Internet is being highly used to reach and abuse children sexually. The Internet is very fast becoming a household commodity in India. Its explosion has made the children a possible victim to the cyber-crime. The pedophiles use their false identity to trap children and even contact them in various chat rooms where they be friend them and gain personal information. They even start contacting children on their e-mail addresses. These pedophiles drag children to the net for the purpose of sexual attack or so as to use them as a sex object.

(v) Accessing Protected System : Any illegal person who secure access or attempts to secure access to a save system is liable to be punished with imprisonment and may also be liable to fine.

(vi) Break of Confidentiality: Any person who secures access to any electronic record, book, register, correspondence, information, document without the permission of the person concerned such electronic record, book, register, information, document or other material to any other person shall be responsible I to be punished under the Information Technology Act.

Table 1: General awareness of cyber culture among Indian internet users

General awareness of cyber culture among Indian internet users	Yes	No
1. Use safety tips like filtering emails, locking personal albums and information, personal walls of social networking sites etc.	69.9%	30.1%
2. Share personal information / emotions with virtual friends / chat room partners etc whom you don't know in real life.	74.0%	26.0%
3. Read policy guidelines of social networking sites, ISPs etc.	28.8%	71.1%
4. Use pseudo names.	45.2%	54.8%
5. Believe in controlling free speech while communicating in the cyber space.	37.0%	63.0%
6. Mail back to unknown senders of spam / pornographic / erotic/phishing mails.	37.0%	63.0%
7. Allow others to use one's own email id / profile id /passwords etc.	46.6%	53.4%
8. Knowledge of minimum age to join cyber communities like Facebook, Orkut, Myspace etc.	56.2%	43.8%

2. CYBER CRIMES UNDER THE INFORMATION TECHNOLOGY ACT:

(i) *Data Diddling:* Data diddling is refers to changing of data before or during entry into the computer system. This kind of an attack involves altering the raw data just before a computer processes it and then changing it back after the processing is completed. The NDMC Electricity Billing Fraud Case that took place in 1996 is a typical example. The computer network was used for receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and payment in the bank were exclusively left to a private contractor who was a computer professional. He misappropriated huge amount of funds by manipulating data files to show less receipts and bank remittances.

(ii) Cyber Stalking: Cyber stalking is a crime in which the attacker harasses a victim by using electronic communication, such as e-mail or instant messaging or messages posted to a Web site or a discussion group. Staking can be referred to as the repeated acts of harassment targeting the victim. A cyber stalker relies upon the anonymity afford by the Internet to allow them to stalk their victim without being detected. Stalking may be followed by serious violent acts such as physical harms to the victim. It all depends on the course of conduct of the stalker.

(iii) Cyber-squatting: Cyber-squatting was originally used to describe the act of registering another's trademarked name, the term is commonly used to describe many different forms of bad faith registrations. It is registering, selling or using a domain name with the intent of profiting from the goodwill of someone else's trademark. It generally refers to the practice of buying up domain names that use the names of existing businesses with the intent to sell the names for a profit to those businesses. The main intention is to divert customers from one site to another and use of false registration information about the customer.

(iv) Cyber Defamation: Any derogatory statement is designed to injure a person's business or reputation, constitutes cyber defamation Cyber defamation is not a specific criminal offense, misdemeanor or tort, but rather defamation or slander conducted via digital media, usually through the Internet.

(v) Financial Crimes: This would include cheating, credit card frauds, money laundering etc. such crimes are punishable under both IPC and IT Act.

(vi) Internet Time Theft: The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. You can identify time theft if your Internet time has to be recharged often, despite infrequent usage. This offence is usually covered under IPC and the Indian Telegraph Act.

(vii) Trojan Attack: A Trojan, the program is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

(viii) Forgery: fake currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners. IT is very difficult to control such attacks. For e.g. across the country students buy forged mark sheets for heavy sums to deposit in college.

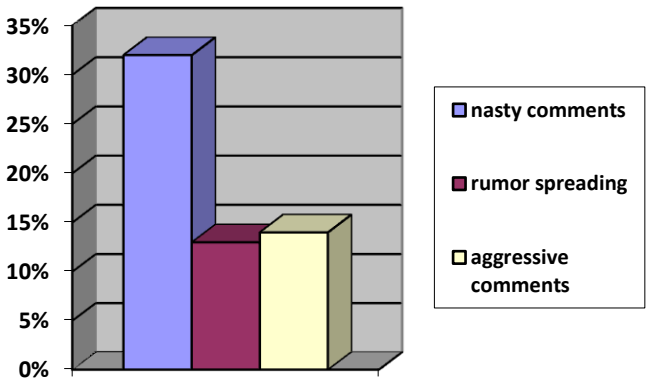
(ix) Virus/worm Attack: Viruses, worms are all part of a class of software called malware. Malware or malicious code (malcode) is short for malicious software. It is code or software that is specifically designed to damage, disrupt, steal, or in general inflict some other "bad" or illegitimate action on data, hosts, or networks. They generally affect the data on a computer, either by altering or deleting it. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

(x) Email Bombing: Email bombing means sending huge amount of mails to the victims as a result of which their account or mail server crashes. The victims of email bombing can vary from individuals to companies and even the email service provider.

3. RESEARCH DESIGN:

A report by the Centers for Disease Control and Prevention (CDC), Electronic Media and Youth Violence: A CDC Issue Brief For Educators and Caregiver . It discusses "electronic aggression," defined as any kind of harassment (including "teasing, telling lies, making fun of someone, making rude or mean comments, spreading rumors, or making threatening or aggressive comments") that occurs through text messaging, email, instant messaging, chat rooms, websites, or blogs. While verbal harassment is the most common form of bullying experienced by young people, followed by physical harassment, electronic aggression is becoming more common because the few studies done to date analyze :-
leading researchers to describe that "10% to 35% of young people say they have been the victim of electronic aggression." Other key findings include:

- the type of electronic aggression most frequently experienced by victims was



- whether rates of harassment differ for boys and girls because some research shows that girls commit electronic aggression more than the boys some studies indicate that electronic aggression may climax around the beginning of high school

- 7% to 14% of youth surveyed reported being a victim as well as a performer of electronic aggression.

- In 2006, 12% of internet users reported being the victim of on-line harassment .

- 1 3% to 46% of young people reported not knowing the identity of the cyber bully .

- Victims of internet harassment are much more likely than non-victims to abuse alcohol .

- Parents who know that their teenager has been a victim of electronic aggression also experience pain, often reporting that they are even more fearful, angry .

- The "vast majority of electronic aggression appears from school grounds but serious consequences for children at school including emotional distress, and feeling unsafe at school.

Suggestions:

Each local and regional board of education shall build and implement a policy to address the existence of harassment in its schools. Such policy shall:

(1) Enable students to secretly report acts of harassment to teachers and school administrators and require students to be notified annually of the process by which they may report.
(2) Enable the parents or guardians of students to file written reports of suspected harassment.
(3) Require teachers and other school staff who witness acts of harassment or receive student reports of bullying to notify school administrators in writing.
(4) Require school administrators to investigate any written reports made under this section and to review.

4. CYBER CRIME OFFENCES ARE DEFINED AS UNDER THESE SECTIONS:

SECTIONS	OFFENCE	PUNISHMENT
43	Damage to Computer system.	Compensation to the tune of Rs. 1 crore to the affected person.
44(a)	For failing to furnish any document, return on report to the Controller or the Certifying Authority.	Penalty not exceeding one lakh and fifty thousand rupees for each such failure.
44(b)	For failing to file any return or furnish any information or other document within the prescribed time.	Penalty not exceeding five thousand rupees for every day during which such failure continues.
44(c)	For not maintaining books of account or records.	Penalty not exceeding ten thousand rupees for every day during which the failure continues.
45	Offences for which no penalty is separately provided.	Compensation not exceeding twenty five thousand rupees to the affected person or a penalty not exceeding twenty five thousand rupees .
65	Tampering with computer source documents.	Imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.
66	Hacking with computer system with the intent or knowledge to cause wrongful loss..	Imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.
66A	For sending offensive messages through communication service etc.	Imprisonment for a term which may extend to three years and with fine.

66B	For dishonestly receiving stolen computer resource or communication device.	Imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees .
67	Publication of obscene material in an electronic form.	Imprisonment up to 5 years and with fine which may extend to one lakh rupees on first conviction and its double punishment for second and subsequent convictions .
68	For failing to comply with the directions of the Controller.	Imprisonment up to 3 years and fine up to two lakhs, or both.
69	For failing to extend facilities to decrypt information which is against the interest of sovereignty or integrity of India.	Imprisonment which may extend to seven years.
70	Securing or attempting to secure access to a protected system.	Imprisonment which may extend to 10 years and fine.
71	For misrepresentation or suppression of any material fact from the Controller or the Certifying Authority.	Imprisonment up to 2 years, or fine up to rupees one lakh or with both.
72	For break of confidentiality and privacy .	Imprisonment up to two years or fine up to rupees one lakh, or with both.

5. PREVENTIVE APPROACH OF CYBER CRIME:

Prevention is better than cure. It is always better to take certain precaution while using the internet.so always follow these preventive approach of cyber-crime.

1. Use of firewalls may be beneficial.
2. Use encryption for your most sensitive files such as tax returns or financial records, make regular back-ups of all your important data, and store it in another location
3. Be aware that your mobile device is vulnerable to viruses and hackers. Download applications from trusted sources.
4. Always Use Strong Passwords So we use different user ID / password combinations for different accounts and a void writing them down. Make the passwords more complicated by combining letters, numbers, special characters (minimum 10 characters in total) and change them on a regular basis.
5. Always use secure wireless network. Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Public Wi-Fi, a.k.a. “Hot Spots”, are also vulnerable. Avoid conducting financial or corporate transactions on these networks.
6. Always use latest and update antivirus software to guard against virus attacks.
7. Never send your credit card number to any site that is not secured, to guard against frauds.
8. Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
9. Prevent spyware from infiltrating your computer by installing and updating anti-spyware software.
10. Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.

6. CONCLUSION:

The fast advancement of Internet and Computer technology has led to the growth of transnational crime especially Internet related. Cyber-crimes have become everywhere today. Internet users must understand that what is offensive in the real space, must be maintained as offensive in the cyber space .The motive behind most cyber-crimes remains the same as that of physical crimes although the technical means to execute them different manner . This

paper we provide some approach to prevent the various cyber-crimes. Thus, there is a need for awareness and performing of necessary legislation in all countries for the prevention of computer related crime. So this kind of crime not solved fully by establishing different law, also need to develop human morality, value and ethics proper manner.

REFERENCES:

1. Adv. Prashant Mali, "Types of cyber-crimes & cyber law in India", CSI Communication, Vol. 35, issue 8, pp. 33-34, November 2011.
2. Ajeet Singh Poonia, Dr.Awadesh Bhardwaj, Dr. G.S Dangayach. Cyber Crime: Practices and Policies for Its Prevention,
3. The First International Conference on Interdisciplinary Research and Development, 31 May - 1 June 2011,
4. Apurba Kumar Roy, Role of Cyber Law and its Usefulness in Indian IT Industry,
5. Eric Knight, Computer Vulnerabilities, CISSP, Electronic Edition, March 2000, release 4.
6. Ghosh, A. K.; Wanken, J.; Charron, F. (1998). Detecting Anomalous and Unknown Intrusions against Programs. In
7. Proceedings of the Annual Computer Security Applications Conference (ACSAC'98), pp.-259-267, Scottsdale, AZ.
8. Zhou, J.; Heckman, M.; Reynolds, B.; Carlson, A.; Bishop, M. (2007). Modeling network intrusion detection alerts for correlation. ACM Transactions on Information and System Security (TISSEC), Volume 10, Issue 1, pp.-1-31.
9. Sommer, R.; Paxson, V (2003). Enhancing byte-level network intrusion detection signatures with context. In: Proceedings of the 10th ACM conference on Computer and Communications Security, ACM, pp. 262-271.
10. Taraq Hussain, Cyber Laws: provisions and preventions.
11. S. Hinde, "The law, cybercrime
12. Cyber Law, Morals & Ethics.

Websites:

www.cybervictims.org
www.cyberlawportal.com
www. cyberlaws india. Net
www. cyberlaws india. Net
www.cyberlawassociation.com.
www.cyberlawonline.com.
www.asianlaw.org/cyberlaw/library/index.html.
www.indii.org/cyberlaw.aspx.
www.cyberlawcentral.com.
www.cyberlawenforcement.org.