International Journal of Law
ISSN: 2455-2194
Impact Factor: RJIF 5.12
www.lawjournals.org
Volume 4; Issue 2; March 2018; Page No. 59-62

Cyber crime and judicial perspective with special reference to bank frauds

Dr. P Ashokkumar
B.Sc, ML. P.hd, Principal, Vasantarao Pawar Law College, Baramati, Maharashtra, India

Abstract
Cybercrime is the crime in which computer is the object of the crime. Common types of cybercrimes includes on line bank information theft, identity theft, Due to this consequences of cybercrimes there was need to adopt a strict law by the cyberspace authority. Cybercrimes can be basically divided into four categories. The cyber laws passed in India are Information Technology Act 2005, Indian Penal Code, Indian Evidence Act. Computer crimes are having drastic effect, on the world in which we live. Though judiciary is protecting the victim rights who are getting prey of hackers, of banks frauds new developing trends to cyber-crime need strict laws and strict punishments for such offences.

Keywords: cybercrime cyberspace, bank frauds

1. Introduction

To define cybercrime, we can say, it is just a combination of crime and computer. To put it in simple terms any offence or crime in which a computer is used is a cybercrime'

Cybercrime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity.

The Cyber crime can halt any railway where it is, it may misguide the planes on its flight by misguiding with wrong signals, it may cause any important military data to fall in the hands of foreign countries, and it may halt e-media and every system can collapse within a fraction of seconds [1].

Definition - What does Cybercrime Mean

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets, or use the Internet fbr exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.

Common types of cybercrime include online bank information theft, identity theft, online predatory crimes and unauthorized computer access. More serious crimes like cyberterrorism are also of significant concern [2].

Cybercrime encompasses a wide range of activities, but these can generally be broken into two categories:

- Crimes that target computer networks or devices. These types of crimes include viruses and denial-of-service (DoS) attacks.
- Crimes that use computer networks to advance other criminal activities. These types of crimes include cyberstalking, phishing and fraud or identity theft.

History

The first recorded cyber crime took place in the year 1820 which is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of

Modern computers, however, began with the analytical engine of Charles Babbage. In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This was the first recorded cyber-crime [3].

Need for Cyber Laws

Information technology has spread throughout the world. The computer is used in each and every sector wherein cyberspace

[1] Sumanjit Das and Tapaswini Nayak, *IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES*, International Journal of Engineering Sciences & Emerging Technologies, 142, (2013), available at http://www.ijeset.com/media/0002/2N12-1JESET0602134A-v6-iss2-142-153.pdf, last seen on 01/10/2013

[2] *Cybercrime*, Techopedia, https://www.techopedia.ccm/definition/2387/cybercrime, visited on 28/09/2016

[3] Er. Harpreet Singh Dalla, Ms. Geeta, *Cyber Crime — A Threat to Persons, Property, Government and Societies*, Volume 3, International Journal of Advanced Research in Computer Science and Software Engineering, 997 (2013), available at www.ijarcsse.com/docs/papers/Volume_3/5_May2013/V315-0374.pdf, last seen on 30/09/2016

provides equal opportunities to all for economic growth and human development. As the user of cyberspace grows increasingly diverse and the range of online interaction expands, there is expansion in the cyber crimes i.e. breach of online contracts, perpetration of online torts and crimes etc. Due to these consequences there was need to adopt a strict law by the cyber space authority to regulate criminal activities relating to cyber and to provide better administration of justice to the victim of cyber crime. In the modern cyber technology world it is very much necessary to regulate cyber crimes and most importantly cyber law should be made stricter in the case of cyber terrorism and hackers [4].

Categories of Cyber Crime

Further Cybercrimes can be basically divided in*to four major categories:*

A) Cyber crimes against persons.

Cyber crimes committed against persons include various crimes like transmission of child-pornography, cyber porn, harassment of a person using a computer such as through e-mail, fake escrow scams.

Cyber-harassment is a distinct Cyber crime. Various kinds of harassment can and do occur in cyberspace, or through the use of cyberspace. Different types of harassment can be sexual, racial, religious, or other. There are certain offences which affect the personality of individuals can be defined as:

1. **Harassment via E-Mails:** Harassment through sending letters, attachments of files & folders i.e. via e-mails.
2. **Cyber-Stalking:** It is expressed or implied a physical threat through use of internet, e-mail, phones, text messages, webcam, websites or videos.
3. **Defamation:** Intent to lower down the dignity of a person by hacking his mail account and sending vulgar mails to unknown persons mail account.
4. **Hacking:** It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programs. Sections 43, 66, 66A, 66C, 67, 67A and 67B of IT Act2008 deals hacking.
5. **Theft of Confidential Information** [Sections 43, 66, 66B of IT Act and Section 426 of Indian Penal Code] ; Many business organizations store their confidential information in computer systems. This information is targeted by rivals, criminals and disgruntled employees.
6. **Spam and Phishing** [Section 66, 66A and 66D of IT Act and Section 420 of IPC] : Spain is basically unwanted emails and messages. Phishing is a method where cyber criminals offer bait so that you take it and give out the information they want. The bait can be in form of a business proposal, announcement of a lottery to which you never subscribed, and anything that promises you money for nothing or a small favor.
7. **E-Mail Spoofing:** A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates.
8. **Carding:** Cloned ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account.
9. **Child Pornography:** Create, distribute, or access materials that sexually exploit underage children.
10. **Assault by Threat: It refers** to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones [5].
11. **Identity Theft:** A major problem with people using the Internet for banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card and other sensitive information to siphon money or to buy things online in the victim's name [6].

B) Cyber Crimes against Property

The second category of **Cyber-**crimes is that of Cyber crimes against all forms of property. These crimes include computer vandalism (destruction of others' property) and transmission of harmful viruses or programs - which are as follows:

1. **Intellectual Property Crimes:** The most common type of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.
2. **Cyber Squatting:** It involves two persons claiming for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously.
3. **Cyber Vandalism:** Vandalism means deliberately damaging property of another. Thus cyber vandalism means destroying or damaging the data or information stored in computer when a network service is stopped or disrupted.
4. **Hacking Computer System:** Hackers attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer.
5. **Transmitting Virus:** Viruses are programs written by programmers that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network.
6. **Cyber Trespass:** It means to access someone's computer or network without the right authorization of the owner and disturb, alter, misuse, or damage data or system by using wireless internet connection.
7. **Internet Time Thefts:** To get 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 [7].

[4] *CYBER CRIMES AND THE LAW*, Legal India News and Law resource portal, available at http://www.legalindia.com/cyber-crimes-and-the-law/, last seen on 01/10/2016

[5] Er. Harpreet Singh Dalla, Ms. Geeta, Cyber Crime —*A Threat to Persons, Property, Government and Societies,* Volume 3, International Journal of Advanced Research in Computer Science and Software Engineering, 999 (2013), available at www.ijarcsse.com/docs/papers/Volume_3/5_May2013/V315-0374.pdf, last seen on 30/09/2016

[6] *Cyber Crime,* Cross Domain Solutions Ensuring Complete Data Security, available at http://www.crossdomainsolutions.com/cyber-crime/, last ssen on 30/09/2016

[7] Er. Harpreet Singh Dalla, Ms. Geeta, *Cyber Crime — A Threat to Persons, Property, Government and Societies,* Volume 3, International Journal of Advanced Research in Computer Science and Software Engineering, 999 (2013), available at

C) Cyber crimes against government

The third category of Cyber-crimes relates to Cyber crimes against Government. Cyber terrorism is one distinct kind of crime in this category. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website.

D) Cybercrimes against Society at large

An unlawful act **done with the** intention of causing harm to the cyberspace will affect large number of persons. These offences include:

1. **Child Pornography:** In this act there is use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity [8].
2. **Cyber Trafficking:** It involves trafficking in drugs, human beings, arms weapons etc. which affects large number of persons. Trafficking in the cybercrime is also a gravest crime.
3. **Online Gambling:** Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. In India a lot of betting and gambling is done on the name of cricket through computer and internet.
4. **Financial Crimes:** Culprit tries to attack by sending bogus mails or messages through internet. Ex: Using credit cards by obtaining password illegally.
5. **Forgery:** It means to deceive large number of persons by sending threatening mails as online business transactions are becoming the habitual need of today's life style [9].

India had enacted its first Cyber Law through IT Act 2000. It has been amended and now in 2008 the revised version is under implementation.

Cyber Laws in India

The following Act, Rules and Regulations are covered under cyber laws:

1. **Information Technology Act, 2000:** The primary source of cyber law in India is the **Information Technology Act, 2000 (IT Act)** which came into force on 17 October 2000. Section 66A of **the IT** Act attempts to address this situation by penalizing the sending of:
   - **i)** any message which is grossly offensive or has a menacing character
   - **ii)** false information for the purpose of causing annoyance. inconvenience. danger, insult, criminal intimidation, enmity, hatred or
   - **iii)** any electronic e-mail for the purpose of causing annoyance or inconvenience, or to deceive the addressee about the origin of such messages;

This offence is punishable with imprisonment upto three years and with a line

The IT Act also penalizes various cyber crimes and provides strict punishments (imprisonment terms upto 10 years and compensation up to Rs 1 crore).

1. **The IT Act was amended by the Negotiable Instruments (Amendments and Miscellaneous Provisions) Act, 2002.** This introduced the concept of electronic cheques and truncated cheques.
2. **Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004** has provided the necessary legal framework for filing of documents with the Government as well as issue of licenses by the Government. It also provides for payment and receipt of fees in relation to the Government bodies.
3. **The Indian Penal Code** (as amended by the IT Act) penalizes several cyber crimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc.
4. Digital Evidence is to be collected and proven in court as per the provisions of the **Indian Evidence Act (as amended by the IT Act).**
5. In case of bank records, the provisions of the **Bankers' Book Evidence Act** (as **amended by the IT Act)** are relevant. Investigation and adjudication of cyber crimes is done in accordance with the provisions of the Code of Criminal Procedure and the IT Act.

Preventive Measures for Cyber Crimes

Prevention is always better than cure. People should take certain precautions while operating the internet and should follow certain preventive' measures for cyber crimes which can be defined as [10].

a) One should avoid disclosing any personal information to strangers via e-mail or while chatting. One must avoid sending any photograph to strangers by online as misusing of photograph incidents increasing day by day.
b) An update Anti-virus software to guard against virus attacks should be used and should also keep a back up so as to avoid data loss in case of virus contamination.
c) Never send credit / debit card number and CVV no to any unsecured site, to guard against frauds.
d) Parents should keep a watch on the sites children are accessing, to prevent any kind of harassment in children.
e) Website owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt some policy for preventing cyber crimes as number of internet users are growing day by day. Web servers running public sites must be physically separately protected from internal corporate network.

Conclusions

In conclusion, computer crime does have a drastic effect on the world in which we live. It affects every person no matter where they are from. It is ironic that those who in secret break into computers across the world for enjoyment have been

www.ijarcsse.com/docs/papers/Volume_3/S_May2013/V315-0374.pdf, last seen on 30/09/2016

[8] *CYBER CRIMES AND THE LAW*, Legal India News and Law resource portal, available at http://www.legalindia.com/cyber-crimes-and-the-law/, last seen on 26/09/2016

[9] Er. Harpreet Singh Dalla, Ms. Geeta, *Cyber Crime —A Threat to Persons, Property, Government and Societies,* Volume 3, International Journal of Advanced Research in Computer Science and Software Engineering, 1000 (2013), available at www.ijarcsse.com/docs/papers/Volume_3/5_May2013/V315-0374.pdf, last seen on 30/09/2016

[10] *CYBER CRIMES AND THE LAW*, Legal India News and Law resource portal, available at http://www.legalindia.com/cyber-crimes-and-the-law/, last seen on 26/09/2016

labeled as deviance. Luckily, the government is making an effort to control the Internet. Yet, true control over the Internet is impossible. Most of the recorded computer crimes cases in most organization involve more than individual and virtually all computer crime cases known so far are committed by employer of the organization. Though judiciary as a guardian is protecting the victims right who are getting prey of hackers of bank frauds, new developing trends in cybercrime need strict laws and strict punishment for such offenses.

References

1. Cyber crime and cyber law -by r.k.chaubey
2. Cyber law and its applications –by donge & shilpa
3. Cyber law in india –by ahmed & farooq
4. Cyber law &commerce –by tayal vimalendu
5. Cyber law –by slingh yatindra
6. Cyber law – by barkha