COMPUTER FRAUDS AND CYBER CRIME: A MIXTURE OF TRADITIONAL AND MODERN

Arpana*

Dr.Meenal Chauhan**

ABSTRACT

Cyber crime is emerging as a serious threat worldwide. Governments, police departments and intelligence units have started reacting. Initiatives to curb cross border cyber threats are taking shape. Indian police has initiated special cyber cells across the country and have started educating the personnel. High level of insecurity on the internet is becoming worrisome so much that transaction on the web has become a thing of doubt. The location and trans-national character of these crimes again added the flavor makes it too dangerous to imagine. This paper explains the concept of cyber-crime, tools being used by the criminals to perpetrate their evil handiworks, identify reasons for cyber-crime, how it can be eradicated and the comparison of cyber crime over the traditional crime.

Keywords: *Cyber insecurity; information; Internet; technology;*

*Lecturer, GJIMT, Ph-II, Mohali, India.

**Assistant Professor, GJIMT, Ph-II, Mohali, India.

INTRODUCTION

Over the past twenty years, unscrupulous computer users have continued to use the computer to commit crimes; this has greatly fascinated people and evoked a mixed feeling of admiration and fear. History reveals that the Cyber crime originated even from the year 1820. That 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. [1]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 is the first recorded cyber crime! This phenomenon has seen sophisticated and unprecedented increase recently and has called for quick response in providing laws that would protect the cyber space and its users. Rapid industrialization and urbanization has brought new forms of crimes involving wider concerns of social order, safety, and security. Thus the present generation greatly depends upon the computer technology for the easy mechanism and effective operations operated in electric format through computers. Though it makes the life so speedy and fast, but hurled under the eclipse of threat from the deadliest type of criminality termed as 'Cyber crime'. Therefore, it is necessary to examine the deadliest form of criminality of the present millennium, conceptually termed as ‘Cyber crime’.

METHODOLOGY

This study was carried out purposely to explain clearly the concept of Cybercrime and Cyber security and provide adequate and sufficient ways of getting out of these problems in the present days of internet usage and applications. The instruments used were observation, and information on the internet as well as report from electronic media.

DEFINITION OF CYBER – CRIME

The term 'cyber crime' has not been defined in any Statute or Act.

[2]The Oxford Reference Online defines 'cyber crime' as crime committed over the Internet.

[3]The Encyclopedia Britannica defines 'cyber crime' as any crime that is committed by means of special knowledge or expert use of computer technology.

[4]CBI Manual defines cyber crime as:

(i) Crimes committed by using computers as a means, including conventional crimes.

(ii) Crimes in which computers are targets.

[5]The Information Technology Act, 2000, does not define the term 'cyber crime'. Cyber crime can generally defined as a criminal activity in which information technology systems are the means used for the commission of the crime.

So what exactly is Cyber Crime? Cyber Crime could reasonably include a wide variety of criminal offences and activities. A generalized definition of cyber crime may be "unlawful acts wherein the computer is either a tool or target or both".

Based on the [6]Director of Computer Crime Research Centre (CCRC) during an interview on the 27th April, 2004, is that "cyber-crime ('computer crime') is any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

Cyber Crimes - Three categories:

- Against Property – Financial crimes – cheating on-line – illegal funds transfer.
- Against Persons – On-line harassment, Cyber Stalking, Obscenity.
- Against Nations – Cyber Terrorism – Damaging critical information infrastructures.

Those involved in committing cyber-crimes are in three categories and they are:

- **THE IDEALISTS (Teenager).** They are usually not highly trained or skilful, but youngsters between the ages of 13 – 26 who seek social recognition. They want to be in the spotlight of the media. Their actions are globally damageable but individually negligible.
- **THE GREED – MOTIVATED (Career Criminals).** This type of cyber-criminals is dangerous because they are usually unscrupulous and are ready to commit any type of crime, as long as it brings money to them. They are usually very smart and organized and they know how to escape the law enforcement agencies.
- **THE CYBER – TERRORISTS.** They are the newest and most dangerous group. Their primary motive is not just money but also a specific cause they defend. They usually engage in sending threat mails, destroying data stored in mainly government information systems just to score their point. The threat of cyber-terrorism can be compared to those of nuclear, bacteriological or chemical weapon threats.

TYPES AND TOOLS USED IN CYBER-CRIME

I. OFFENSIVE MESSAGES

(Messaging, annoying, intimidating, insulting, misleading, defaming)

a) SMS

SMS of above nature may be sent using mobile phone of one's own identity or by acquiring a fade identity. Such SMS may be forwarded amongst groups and communities (inter/intra) in which case the actual source could not be fixed. Few SMSs had been circulated affecting public tranquility; Eg: False Tsunami warning, false alarm as target of explosion.

b) MMS

Multimedia messages often defaming or obscene are sent among small groups using mobile phones/Bluetooth If there had been a sharing in many mobile equipments the first source couldn't be fixed. Eg: Arrest of the Managing Director of bazee.com in a school MMS scandal in Delhi.

c) Web based SMS

SMS can be sent by logging onto sites like way2sms.com by becoming a member of the site typing the message of choice and choosing destination to be sent anywhere in the world by concealing one's identity.Way2sms never share the IP logs with law enforcement agencies.

d) Chat room messages

Chat room messages in internet relay chats happens by direct connection between each others' machines in which the IP logs are stored neither by Yahoo nor Google and so information shared in Chat rooms may be saved but can never be traced retrospectively to its origin.

II OFFENSIVE CALLS

(Offender calls either by his/her own name or by acquiring false identity- Landline calls/mobile calls, web based calls, VOIP calls, Skype, Yahoo messenger, Chat room calls, overseas calls etc.)

a) Landline/mobile calls

Many landlines still have no caller Ids. Difficulty if the connection is in a non-existent fictitious address.

b) Web based calls

Calls can be made by spoofing the mobile number using the sites like http://www.phonetrick.net/, http://www.prankdial.com/

c) Overseas calls Landline/mobile

For overseas landline/mobiles the details of the subscribers are not available without the co-operation of international agencies.

d) Chatroom calls – VOIP Calls – Skype

In VOIP it is difficult to ascertain the source as it passes through various international gateways before it enters the country to get terminated in an Indian operator's subscriber

III Deceptive messages (Lottery, cheating, job racket)

(*SMS of lottery cheating, emails of prize money, articles, false promise of jobs, false mail for admission to a reputed University)*

- Greed of the victim is the main reason why cyber frauds are successful.
- SMS/Email messages of winning a lottery of prize money or articles, alluring people to deposit money.
- Clues available are email IDs and sometimes few mobile phone numbers.
- Live.com, Yahoo.co.uk domains IP which are frequently used never share the login IPs and it provides a conducive climate for commission of crimes.
- To the extent it was made available, the IP logs invariably had shown some Nigerian, Mediterranean, Middle East and American countries. Hence users details are not available.
- The mobile numbers are often fictitious and seasonal.
- The Bank accounts are invariably bogus and have transient life; sometimes an innocent gets allured for commission by stating false reasons for the source of money.
- The following awareness messages have been propagated:
  - ❖ Do not believe emails or SMS that say that you have won a million dollar lottery.
  - ❖ Be way of strangers who promise to transfer Crores of rupees to your bank account.
- Similar cheating can be for prize of cars, for an employment to a job fetching high income, admission to a course in a reputed university abroad.
- Sometimes Nigerians use the tool of threat of an insider staying inside star hotels waiting for instructions to ignite an explosive if not parted with the ransom money by negotiations.
- Occasionally criminals hide behind proxy servers by concealing their real location of log-ins.
- (Threat to critical infrastructures and vital installations and public places) E-mails of threatening nature often with an intention to mislead or to deceive or to implicate another person by wielding threat to critical infrastructures.

IV. DATA THEFT

(Theft of proprietary information causing breach of confidentiality and integrity and thereby altering its utility value. More due to disharmony in employee/employer situations by disgruntled employees.)

- Sensitive information belonging to business organizations is targeted by rivals, criminals and sometimes even by disgruntled employees.
- Disharmony in work place often makes the ex-employees to take away the valuable data or design or client information.
- Sometimes they damage it; delete it; or sell it to a competitor.
- Many a times the employers become suspicious about their ex-employees and attribute instances of data theft which the ex-employee was holding in his possession to carry out his official duties at the time of his employment.
- Frequently breach of Non Disclosure of Agreement (NDA) and Memorandum of terms of employment are often attributed to criminal activity by employers which in truth may be a civil violation.

V. IDENTITY THEFT

- Identity theft involves fraudulent or dishonest use of someone's electronic signature, password or other unique identification feature.
- It is the first step towards credit card fraud, online share trading scams and e-banking crimes.

VI. INTERNET VIOLATIONS OF COPY RIGHTS

(Internet violation of copyrighted information's like feature films, songs, music etc. IPR theft)

- Posting of features films, part of the films, causing loss to the revenue and criminal violations of Copy Right Act, 1957 often challenges the film industries and law enforcement.
- Uploading happening in Indian servers can be deleted.
- If it is an International server, deletion happens by request. Despite that if persisting, deletion becomes a task of chance and persons behind the activity may not surface at all.

VII. FINANCIAL CRIMES –SPOOFING/PHISHIHG/INTERNET BANKING

(Offender creates/Spoofs the webpage of a bank or any organization in the guise of enhancing their security or updating the services, collects personal confidential information at various stages and abuses the information for causing wrongful loss, fraudulent transfer of

funds in Internet banking. This is a wide term that includes credit card fraud, online share trading scams and e-banking crimes.)

- In today's highly digitalized world, almost everyone is affected by financial crimes.
- Phishing usually involves spoofed emails that contain links to fake websites.
- Spoofing becomes a pre-requisite for causing deceptive belief and it follows phishing of vital information.
- Spoofing of the sites normally happens in bank pages if the intention is for a financial fraud. Other sites get spoofed for misleading the viewer or for causing embarrassment.
- A spoofed page becomes difficult to be distinguished by normal viewers.
- Phishing normally happens for credit card related information or for password details of internet banking.
- Internet Banking requires unique authentication. Forgotten PIN or password option generates new ones if answers to the questions match. New PIN or Passwords reach as mobile SMS, mobile phone security if compromised, criminals then know the precious PIN or Password.
- Fund transfer normally goes to bogus fictitious accounts within the country but far apart in Geography.
- Quick withdrawal happens through short living accounts and the offender manages to open further bogus accounts as a preparation for his future crimes.
- Withdrawal happens mostly in ATMs by concealing the identity.
- Banking systems and mobile phone systems provide facilities without proportionate security breeding vulnerabilities.
- The system now is not immune for account opening or for activating a new SIM card by producing forged ID cards and non-existence characters or by impersonation.
- Sheer non-compliance of the KYC norms of RBI and verification norms of TRAI opens wide scope for criminal activities ranging from a disturbance call to a fraudulent fund transfer culminating even as a mean for anti-national activities.
- The following awareness message have been Propagated:
  - ❖ Never respond to unsolicited emails asking for financial information

VIII. WEB PAGE HACKING

(The page gets defaced by altering the content of the file and appearance causin embarrassment and denial of service)

- The primary objective in web page hacking is to deface and embarrass an organization or an institute.
- The intention may extend from causing a denial of service to bringing down a business competitor.
- Government sites get hacked and hackers sometimes claim responsibility for hacking; the intention being to cause defamation and damage to the dignity of the institution.

IX. SPAM/MALWARE/ ESPIONAGE

- Spam is the abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately.
- E-mail spam, known as junk mail, is the practice of sending unwanted email messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients.
- Malware is software designed to infiltrate or damage a computer system without the owner's informed consent.
- Malware is a wide term that includes viruses, worms, Trojans, rootkits, backdoors, spyware, botnets, keystroke loggers and dialers.
- Cyber espionage is the act of obtaining personal, sensitive proprietary or classified information without permission.
- Also known as cyber spying, it involves the use of cracking techniques and malicious software including Trojans and spyware.

X. MOBILE DEVICE ATTACKS

- Threats to the security of mobile devices include unauthorized access, stolen, handsets, data theft, malware, phishing etc.
- Mobile devices are getting more computing power and are becoming increasingly feature rich. This increases the likelihood of attacks against potential vulnerabilities.

XI. DENIAL OF SERVICE

- This involves flooding a computer with more requests than it can handle, causing it to crash.
- In a Distributed Denial of Service (DDoS) attack, the perpetrators are many and are geographically widespread.

XII. SOCIAL ENGINEERING

- A social engineering attack tricks people into revealing passwords or other confidential information by making people believe an unanticipated situation.

- Training the personnel for handling such situations and effectively ensuring the "need to know basis" may be a viable solution.

XIII. VIOLATION OF PRIVACY

(Capturing and publishing the images, pictures and videos of individuals often without the knowledge and concurrence and thereby passing humiliation and embarrassment)

- Normally females victimized in this way by the posting of pictures with an attachment of an unwanted message, often with the phone number to cause incessant disturbance by calls from international strangers.
- Social networking sites like Orkut have fairly responded to Police requests by furnishing the IP addresses and log details.
- Face book has proved to be a non-responsive, despite requests not withstanding even if addressed to any of the International organizations like Child Exploitation On-line Protection forums.
- Social networking sites like face book have maintained its unbroken silence if requests for deletion of posted pictures were addressed.

XIV. CYBER TERRORISM

- Cyber terrorism involves the use or threat of disruptive cyber activities for ideological, religious or political objectives.
- Cyber terrorism can weaken a country's economy and even make it more vulnerable to military attack.

XV. OBSCENITY & PORNOGRAPHY

(Uploading obscene and lascivious materials in Internet and causing propagation and transmission: abusing children and uploading of images of such abuse).

- International online sharing sites like Rapidshare, megaupload and various sites have provided a nurturing platform for the cultivation, propagation and transmission of the menace of pornography including children.
- Surprisingly sites like Paypal and other online payment sites have been hand in glove with such sites prompting one to infer that there might be a sharing of the proceeds of income by the propagation of pornography.
- Blocking of porno-sites had been a challenge both in technical and legal means because the content can be hosted in a different domain names or in different IP addresses from different geographies of the world.

HOW TO ERADICATE CYBER – CRIME

Research has shown that no law can be put in place to effectively eradicate the scourge of cyber-crime. Attempts have been made locally and internationally, but these laws still have shot-comings. What constitutes a crime in a country may not in another, so this has always made it easy for cyber criminals to go free after being caught.

These challenges notwithstanding, governments should in the case of the idealists, fight them through education not law. It has been proven that they help big companies and government see security holes which career criminals or even cyber-terrorist could use to attack them in future. Most often, companies engage them as consultants to help them build solid security for their systems and data. The use of passwords, firewalls, encryption, security policies and procedures are some preventive measures against cybercrime. Detection techniques include tripwires, configuration-checking tools, and anomaly detection systems. A tripwire is a software program that takes snapshots of critical system characteristics that can be used to detect critical file changes. Tripwires provide evidence of electronic crimes, since most intruding hackers make modifications when they install backdoor entry points or alter file system and directory characteristics in the course of hacking system. A configuration-checking tool, also referred to as a "vulnerability assessment tool," is a software program that detects insecure systems. Configuration-checking tools are primarily preventive in nature but, when used as monitoring devices, they can also provide evidence regarding electronic crimes.

Another means of eradicating cyber-crime is to harmonize international cooperation and law, this goes for the greed motivated and cyber-terrorists. They cannot be fought by education, because they are already established criminals. The only appropriate way to fight them is by enacting new laws, harmonize international legislations and encourage coordination and cooperation between national law enforcement agencies.

CYBER-CRIME- MIXTURE OF TRADITIONAL AND MODERN

i. Incidences of Traditional crime - easy to deal

The incidence of traditional crime, most of the time, is easy to deal by law regulating agency. Here location can be traced out, person can be identified, facts and issues can be investigated, telephone calls can be scrutinized and liability can be imposed.

Demarcation between Cyber-crime and that of so called traditional crime can be traced out on some distinguished footings.

ii. Incidences of Cyber Criminality

Relatively, in case of Cyber-criminality, Cyber space allows these attacks easily carry out and such intrusions can be made effortlessly with very little risk of apprehension. First of all, it is very difficult to fix the identity to the perpetrator in Cyber-space as it is very easy to mask a fake identity. You can have a mask of famous hero, heroin, politician or even policeman with photo-identify in the Cyber-space. It is difficult to see the person actually sitting in front of terminals and only the manifested identity is only source in Cyberspace. Secondly, it is difficult to locate the jurisdiction and locality of the perpetrator. Neither it possible his intentions and benefit he receive from such deviation.

iii. The fashion of 'Computer literacy' fasten the process of Cyberisation

Today the courses pertaining to ‘computer literacy’ training become an integral part of curriculum. Due to the vast use of electronic devices within the atmosphere available around the new generation, the new generation very easily got electronic indoctrination. Due to tender age and lack of judgment capability there are equal chances of their exposure to the evil effect of this technology.

iv. Cyber Crime - Neither difficult to learn nor difficult to commit

Cyber-crime is neither much hard to learn nor much difficult to commit. In modern society, computer technology can be learned like language. Particularly, the new generation for whom computer knowledge is an essential part of curriculum, and where knowledge diffusion is with the help of computer it is very easy for them to have convenience accessible means to commit crime in Cyber-space. Today, anybody with minimum computer literacy is sufficient to have access to Cyber-criminality and the chances are very less of being trapped by the preventive agencies. These features make Cyber-crimes more dangerous and alarming.

v. Difficulties in tracing the Cyber crime

If one is enough fortunate to overcome these difficulties of locating, investigating and fixing the criminal liability, the next complexities he has to face about the collection, examination, scrutiny, instigation and recording and reading the evidences and witnesses.

In short, such problems make Cyber-criminality more severe and serious in this millennium. In addition to that, as due to Internet facilities, Cyberspace don't recognized boundaries, barriers or line of control of the nations, the problem of jurisdiction also create problem in Cyber-criminality.

CYBER-CRIME VERSES TRADITIONAL CRIME

Some of the Cyber crime that appears in Cyber space is resemble with the traditional criminality only with the difference that they are committed in Cyberspace with the help of computers. Some of the Cyber crime that resemble with traditional crime fall in the categories of economic offences.

Therefore, while dealing with the crime similar with old-fashioned crime, only procedure will be different. However, some of the crimes committed in Cyber space are entirely new in varieties, e.g. infringements on privacy, propagation of illegal and harmful content, facilitation of prostitution and other moral offenses, and organized crime. As these crimes involve a complex phenomenon either due to its special type or due to its transnational nature, it requires to be considered on entirely different footings.

CONCLUSION

The 'Technological Adoption' should be scrutinized and introspected with 'Domestic Justification', particularly for developing and underdeveloped community where compelling priority and developmental level differ from western countries. To provide self-protection, organizations should focus on implementing cyber-security plans addressing people, process and technology issues, more resources should be put in to educate employees of organizations on security practices, develop thorough plans for handling sensitive data, records and transactions and incorporate robust security technology- -such as firewalls, anti-virus software, intrusion detection tools and authentication services. This is a time to act, to plan, to get protected the generation, because electronic technology has greater potentiality to destroy society than any other previous variables. Surely, ***if we fail to plan, we plan to fail!!!***

REFERENCES

1. http://cybercrime.planetindia.net/intro.htm
2. http://www.oxfordreference.com
3. www.**cyber**security.my/data/content_files/13/134.pdf
4. www.hcmadras.tn.nic.in/.../**Cyber**%20**Crime**%20by%20KNBJ.pdf
5. nicca.nic.in/pdf/itact2000.pdf
6. www.sans.org/.../international-cybercrime-treaty-ratification_1756
7. Douglas A. Barnes. Deworming the internet. Texas Law Review, 83:279_329, November 2004.
8. Aaron J. Burstein. Towards a culture of cybersecurity research. Harvard Journal of Law and Technology, 22:230_240, 2008.

9. Van J Garcia F, Hoepman J and Nieuwenhuizen J. Proceedings of 19th i_p international information security conference, wcc2004-sec, toulouse, france. In Spam _lter analysis. Kluwer Academic Publishers., 2004.
10. Hammond and Allen. The 2001 council of European convention on cybercrime. In an E_cient Tool to Fight Crimes in Cyber-Space?, June, 2001.
11. http://www.asianlaws.org/press/cybercrime.htm. Cyber crime is here to stay. Indian Express, 4, 2002.
12. Daniel J. Solove and Chris Jay Hoofnagle. A model regime of privacy protection. University of Illinois Law Review, 7:1083_1167, 2002.
13. Berkley l Joseph P, Liu. The dmca and the regulation of scienti_c research. Technology Law Journal, 18:501, 2003.
14. Paulson LD. Spam hits instant messaging. Computer and Internet Security, 37 no 4:18, 2004.
15. Tygar J Rachna D and Marti Hearst. Proceedings of the conference on human factors in computing systems. In Why Phishing Works, 2006.
16. Euguene Volokh. Crime-facilitating speech. Stanford Law Review, 57:1095_1222, March 2005.