RESEARCHERID
THOMSON REUTERS
[INIT: January 2017]
ISSN 2348 – 8034
Impact Factor- 4.022
GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

CYBER CRIME & SECURITY

Uma Chaudhary*
*Lecturer, Department of Commerce & Management BEL First Grade College, Jalahalli, Bangalore

ABSTRACT

In the present day, world has witnessed an unprecedented index of Cyber crimes whether they pertain to Trojan attacks, e-mail bombing, E-Mail Spoofing, DOS attacks, information theft, Fraud or the most common offence of hacking. Despite technological measures being adopted by corporate organizations and individuals, we have witnessed that the frequency of cyber crimes has increased over the last decade. Since users of computer system and internet are increasing worldwide in large number day by day, where it is easy to access any information easily within a few seconds by using internet which is the medium for huge information and a large base of communications around the world.

This study paper highlights various categories of cyber crime and cyber crime as a threat to person, property, government and society. It discusses the cyber laws & current status of cyber crime in India.

The National Crime Records Bureau (NCRB) released their annual "Crime in India" report. The report tracks statistics for various types of crimes across India, and provides useful insight into socio-legal trends, as well as problems being faced by law enforcement agencies in the country.

The NCRB has been tracking statistics relating to cybercrime also. Based on NCRB trackers, Between 2011 and 2015, the country witnessed a surge of nearly 350% in cybercrime cases reported. However, despite an increasing number of cases being reported, conviction rates remain very low. For example, Maharashtra saw only a single conviction in 2015 despite over 2000 cases being registered.

While it is true that convictions are not generally related to the cases filed in the same year, low conviction rates are generally indicative of high pendency of cases, as well as an underdeveloped architecture of investigation and deterrence.

This paper also explains various preventive measures to be taken to snub the cyber crime. Certain precautionary measures should be taken by all of us while using the internet which will assist in challenging this major threat Cyber Crime

Keywords- *Cyber Crime. Computer crime, Hacking, Cyber Fraud, Prevention of Cyber Crime.*

I. INTRODUCTION

The advancement of technology has made man dependent on Internet for all his needs. Internet has given man easy access to everything while sitting at one place. Social networking, online shopping, storing data, gaming, online studying, online jobs, every possible thing that man can think of can be done through the medium of internet. Internet is used in almost every sphere.

With the development of the internet and its related benefits also developed the concept of cyber-crimes. With increasing internet penetration, cyber crimes have also increased in the last few years.

Cyber crimes are committed in different forms. A few years back, there was lack of awareness about the crimes that could be committed through internet. In the matters of cyber crimes, India is also not far behind the other countries where the rate of incidence of cyber crimes is also increasing day by day.

ISSN 2348 – 8034
Impact Factor- 4.022

As preventions, certain precautionary measures should be taken by all of us while using the internet which will assist in challenging this major threat Cyber Crime.

II. WHAT ARE CYBER CRIMES

Cyber crimes can be defined as the unlawful acts where the computer is used either as a tool or a target or both. The term is a general term that covers crimes like phishing, credit card frauds, bank robbery, illegal downloading, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and/or distribution of viruses, Spam and so on.

Cyber crimes are a new class of crimes which are increasing day by day due to extensive use of internet these days.

III. DIFFERENT TYPES OF CYBER

Crimes
Cyber Crimes can be categorized in two ways:

1. ***Computer as target***: These types of crimes are hacking, virus attacks, DOS attack etc.

2. ***Computer as Weapon:*** These types of crimes include cyber terrorism, IPR violations, credit card frauds, pornography etc.

IV. CATEGORIES OF CYBER CRIMES

Cybercrimes can be basically divided into four major categories:

A. Cyber crimes against Persons

This category of Cyber-crimes are committed against individual person.

1. **Unauthorized Access and Hacking:** It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programs. Hackers usually hacks telecommunication and mobile network.

2. **Cracking:** It is act of breaking into your computer systems without your knowledge and consent and has tampered with precious confidential data and information

3. **Carding:** It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account. There is always unauthorized use of ATM cards in this type of cyber crimes.

4. **Cheating & Fraud:** It means the person who is doing the act of cyber crime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.

5. **Defamation**: It involves any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.

6. **Cyber-Stalking:** In general terms, stalking can be termed as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harm to the victim. Cyber Stalking means repeated acts of harassment or threatening

ISSN 2348 – 8034
Impact Factor- 4.022

behaviour of the cyber criminal towards the victim by using internet services. Both kind of Stalkers i.e., Online & Offline – have desire to control the victims life.

7. **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.

8. **Harassment via E-Mails:** This is very common type of harassment through sending letters, attachments of files & folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Facebook, Twitter, Orkut etc. increasing day by day.

9. **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.

B. Cyber crimes against Property

The second category of Cyber-crimes is that of Cyber crimes against all forms of property.

1. **Virus attacks:** These crimes are committed through transmission of harmful viruses or programs. A Mumbai-based upstart engineering company lost a say and much money in the business when the rival company, an industry major, stole the technical database from their computers with the help of a corporate cyber spy software.

2. **Intellectual Property Crimes:** Intellectual property consists of a bunch of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is a crime. 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.

3. **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. For example two similar names i.e. www.yahoo.com and www.yahhoo.com.

4. **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. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral or a device attached to the computer.

5. **Hacking Computer System:** Hackers attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity there will be loss of data as well as computer system. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company. As in April, 2013 MMM India attacked by hackers.

6. **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. They mainly affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computer system of the individuals.

7. **Software Piracy:** Software piracy refers to the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. These kind of crimes also include copyright infringement, trademarks violations, theft of computer source code, patent violations etc.

ISSN 2348 – 8034
Impact Factor- 4.022

C. Cyber crimes 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.

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:** There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering. Cases of hawala transactions and money laundering over the Internet have been reported.

   In India a lot of betting and gambling is done on the name of cricket through computer and internet.

4. **Financial Crimes:** This type of offence is common as there is huge growth in the users of networking sites and phone networking where culprit will try to attack by sending bogus mails or messages through internet. Ex: Using credit cards by obtaining password illegally.

5. **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.

6. Sale of illegal articles: This category of cybercrimes includes sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication.

D. Cyber crimes against Government

The third category of Cyber-crimes relates to Cyber crimes against Government.

1. **Cyber terrorism:** is one distinct kind of crime in this category. The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to threaten the citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website. The Parliament attack in Delhi and the recent Mumbai attack fall under this category.

V. CYBER LAWS & CYBER CRIME IN

INDIA

To combat the crimes related to internet, India had enacted its first Cyber Law through IT Act 2000. Cyber Crimes in India are registered under three broad heads,

- IT Act,
- Indian Penal Code (IPC)
- Other State Level Legislations (SLL)

ISSN 2348 – 8034
Impact Factor- 4.022

Year	IT Act		IPC	
	Cases Registered	Persons Arrested	Cases Registered	Persons Arrested
2011	1791	1184	422	446
2012	2876	1522	601	549
2013	4356	2098	1337	1203
2014	7201	4246	2272	1224
2015	8045	5102	3422	2867
Total	24269	14152	8054	6289

Fig 1: Cyber Crimes in India up by more than 3 times in 5 years

The numbers of cases registered under the IT Act and IPC have been growing continuously. The cases registered under the IT act grew by more than 350% from 2011 to 2015. There was almost a 70% increase in the number of cyber crimes under the IT act between 2013 and 2014.

The cases registered under the IPC increased by more than 7 times during the period between 2011 and 2015. Similar trend is observed in the number of persons arrested.

The government also acknowledges the increase in the number of such crimes and that the introduction of technologies, devices including smart phones and complex applications, and rise in usage of cyber space for businesses has resulted in such an increase.

VI. CYBER- SAFETY ACTIONS

Prevention is always better than cure. It is always better to take certain precautions while working on the net. One should make them a part of his cyber life.

Cyber-safety is a common term used to describe a set of practices, measures and/or actions you can take to protect personal information and your computer from attacks. Few Basic Cyber safety are explained below:

1. **Install OS/Software Updates:**

- Updates (sometimes called patches)-Fix problems with your operating system (OS) (e.g., Windows XP, Windows Vista, Mac OS) and software programs (e.g., Microsoft Office applications).
- Most new OSs are set to download updates by default. After updates are downloaded, you will be asked to install them. Click yes!
- To download patches for your system and software, visit the official websites.
- Be sure to restart your computer after updates are installed so that the patches can be applied immediately.

2. **Run Anti-virus Software**

- To avoid computer problems caused by viruses, install and run an anti-virus programs like AVG, Symantec etc.
- Periodically, check to see if your anti-virus is up to date by opening your anti-virus program and checking the Last updated: date.
- Anti-virus software removes viruses, quarantines and repairs infected files, and can help prevent future viruses.

3. **Prevent Identity Theft**

- Don't give out financial account numbers, Social Security numbers, driving license numbers or other personal identity information unless you know exactly who's receiving it. Protect others people's information as you would your own.

ISSN 2348 – 8034
Impact Factor- 4.022

- Never send personal or confidential information via email or instant messages as these can be easily intercepted.

4. Turn on Personal Firewalls

- Firewalls act as protective barriers between computers and the internet.
- Check your computer's security settings for a built-in personal firewall. If you have one, turn it on. Microsoft Vista and Mac OSX have built-in firewalls.
- Once your firewall is turned on, test your firewall for open ports that could allow in viruses and hackers. Firewall scanners like the one on http://www.auditmypc.com/firewall-test.asp simplify this process.
- Hackers search the Internet by sending out pings (calls) to random computers and wait for responses. Firewalls prevent your computer from responding to these calls.

5. Avoid Spyware/Adware

- Spyware and adware take up memory and can slow down your computer or cause other problems.
- Watch for allusions to spyware and adware in user agreements before installing free software programs. Be wary of invitations to download software from unknown internet sources.

6. Protect Passwords

- Do not share your passwords, and always make new passwords difficult to guess by avoiding dictionary words, and mixing letters, numbers and punctuation.
- Do not use one of these common passwords or any variation of them: qwerty1, abc123, letmein, password1, iloveyou1, (yourname1),
- Change your passwords periodically.
- Store passwords in a safe place. Avoid keeping passwords on a Post-it under your keyboard, on your monitor or in a drawer near your computer!

7. Back up Important Files

- Reduce your risk of losing important files to a virus, computer crash, theft or disaster by creating back-up copies.
- Keep your critical files in one place on your computer's hard drive so you can easily create a back up copy.
- Save copies of your important documents and files to a CD, online back up service, flash or USB drive, or a server.
- Store your back-up media in a secure place away from your computer, in case of fire or theft.
- Test your back up media periodically to make sure the files are accessible and readable.

VII. CONCLUSION

The NCRB report highlights the fact that problems that have plagued most areas of the Indian criminal justice system continue to be issues in relation to cybercrime. These include high pendency of cases, low conviction rates and low reporting.

These problems are exacerbated by rising usage of information technology resources with limited knowledge of good cyber security principles.

Experts have also suggested that the Indian ecosystem around cyber policing is simply not equipped to secure convictions, because of an inadequately trained police force, limited technical resources, low co-ordination between the public and private sector, and an unequipped judicial system.

Government has set up an expert group to formulate appropriate means to tackle growing cybercrime in India. Following this, the government agreed to take various steps, including the establishment of a National Cyber Crime Coordination Centre ("NCCC") in order to focus on cybercrimes and national security issues and ensure appropriate

communication between agencies. Reports have suggested that Phase I of the NCCC will be live by March 2017. It has also been agreed that cybercrime complaints can be filed online without the necessity of visiting a police station.

There have also been other steps taken, including the establishment of cyber labs promising additional technical, and increased emphasis on international co-operation. It is to be hoped that these measures will go a long way towards assuaging the policing problems currently facing cybercrime in India.

REFERENCES

1. *Communications Fraud Control Association. 2011 global fraud loss survey. Available: http://www.cfca.org/fraudlosssurvey/, 2011.*
2. *F. Lorrie, editor. "Proceedings of the Anti-Phishing Working Groups", 2nd Annual eCrime Researchers Summit 2007, Pittsburgh, Pennsylvania, USA, October 4–5, 2007, vol. 269 of ACM International Conference Proceeding Series. ACM, 2007.*
3. *Microsoft Inc. Microsoft security intelligence report, volume 9, 2010. Available: http://www.microsoft.com/security/sir/.*
4. *Windows Update: http://windowsupdate.microsoft.com*
5. *Microsoft Update: http://www.update.microsoft.com/microsoftup date/*
6. *Firewall Testing http://www.auditmypc.com/firewall-test.asp*