Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

The Evolution of Cyber crime and the Attacks that led to the Formation of Cyber Laws in India

Uvika Kujur[1,] Swati Bareth[2]

[1,2,] Department of Comp. Sc. & App., Loyola College Kunkuri
uvikakujur666@gmail.com, swatibareth62@gmail.com
9340950164, 8319125721

ABSTRACT

Nowadays, Cybercrime has caused a lots of deface to an individual, organization and even the government sectors. Many cybercrime detection and classification methods have overcome with various levels of success in order to prevent, protect and authorized data from Cyber-attacks. Cybercrime is that activity done by human being knowingly or unknowingly to ruin organizations network, stealing important data and documents, hacking bank accounts details, transferring money to their own and so own.This paper describes about the common areas where cybercrime usually occurs and also classify various types of cybercrimes and laws to prevent and protect from cyber-attacks. This paper also deals about the main causes of cybercrimes occurred.

Keywords: cybercrime, cyber-attacks, causes, protect, cyber laws

I. INTRODUCTION

Cybercrime is the latest and the most complicated problem in cyber world. The term crime is denoted an unlawful act which is punishable by a state (Ramdinmawaii et al. 2014). Crime is also called as an offense or a Criminal offense. Cyber-criminal use internet and computer technology to hack user's personal Computers, Smartphone data, personal details fromsocial media, national secrets etc. In general. We can define computer as the machine that oar stores and manipulate or process information or instruction, instructed by the users.

The term Cybercrime can be defined as an act of committed or omitted in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction (Saini H. et. al., 2012). The term "Cyber law" doesn't have a fixed definition, but we can defined it as the law that governs the Cyberspace. Cybercrimes, Digital and electronic signatures data protections etc. are comprehended by the cyber law (Saini H. et. al., (2012).The UN'S general assembly recommended the first IT act of India which was based on the "united nations Model law on Electronic commerce "Model(Saini H. et. al., 2012). Cyber law is generic term which refers to all the legal and regulatory aspects of internet. It is a constantly evolving process, if the internet grows, numerous legal issues also arises. Cybercrime may be used of an instrument for an illegal ends of activity such as online gambling, financial crimes, cyber stalking, email spoofing, sales of illegal articles, forgery, committing fraud, violating privacy etc.

I. CYBERCRIME

II. (a) History of Cybercrime

The first Cybercrime was recorded in the year 1820. The ancient type of computer has been in Japan, China, and India. Since 3500 B.C. The era of modern computer began with the analytical engine of Charles Babbage.

US $ 10 million were fraudulently transferred out of the bank and into a bank account in Switzerland. A Russian hacker group led by Vladimir Kevin, a renowned hacker, perpetrated the attack. The group compromised the bank's security systems. Vladimir was allegedly using his office computer at AO Saturn, a computer firm in St. Petersburg Russia, to break into Citibank computers. He was finally arrested on Heathrow airport on his way to Switzerland (Choudhury R. R. et. al., 2013).

The Cybercrime is enlarged from Morris worm to the ransom ware. Several country like America, China, Germany, Britain including India are working to stop such Cybercrimes and attacks, but these attacks are frequently changing and influencing our nations. Here are lists of some types of attacks given below and they are as:

Table No. 1

II. (b) Evolution of Cybercrime

Years	Types of Attacks
1971	A phone phreak
1995	Macro-viruses
1997	Cybercrimes and viruses initiated, that includes Morris code worm and other.
1999	Melissa viruses
2002	Shadow crew's website
2004	Malicious code, Trojans, Advanced worm etc.
2007	Identifying thief, Phishing etc.
2010	DNS Attack, Rise of Botnets, SQL attacks etc.
2013	Social Engineering, DOS Attacks, BotNets, Malicious Emails, Ransomware attack etc.
Present	Banking Malware, Keylogger, Bitcoin wallet, Phone hijacking, Anroid hack, Cyber warfare etc.

II. (c) Types of Cybercrimes

There are many types of cybercrimes and they have been discussed given below

i. Email spoofing
ii. Salami attack
iii. Worm/virus attacks
iv. Web jacking
v. Phishing
vi. Forgery
vii. Online Gambling

i. Email Spoofing: E-mail spoofing basically means sending an email from a source while it appears to have been sent from another source. These tactic are used in phishing and spam campaigns mostly people think that the email has been sent by any legal source and they used to open that email. The mail goal ofemail spoofing is to get recipients to open and possibly even respond to a solicitation. Financial crimes are commonly committed through E-mail spoofing.

ii. Salami attacks: Salami attacks is also known as salami slicing. It is often used to carry out illegal activities, Attackers uses customer online database information like bank details, etc. Attackers reduces very few amounts from every account over a period of time and the customer remains unaware of thisslicing and hence no complain is filled.

iii. Virus/worm attacks: Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to (Dashora K., 2011). They merely make functionalcopies of themselves and do this repeatedly till they eat up all the available space on a computer's memory**.** The world's most famous worm was the internet worm let loose on the internet by Robert Morris sometime in 1988.

iv. Web Jacking: This term Web jacking is derived from the term hi jacking. In these kinds of offensethe attacker creates a fake websites and when the victims opens the link a new page appears with the message and they need to clicks the link that looks real he will redirected to a fake page(Saini H. et. al., 2012). Hence these types attacks are done to get approach or to get access and control the cite of another. The attacker may also change the information of the victim's webpage.

v. Phishing: In Phishing, the attacker's tries to gain information such as login information or passwords, details of credit card, account's information by simulate as a reputable individual or entity in several communication channels or in emails. Phishing e-mails are likely to contain hyperlinks to the sites containing malwares.

vi. Forgery: It means making of false documents, signature, currency, revenue stamp etc.

vii. Online Gambling: It is offered by thousands of websites that have servers hosted abroad. Theses websites are the one of the most important sites for money launderers (Ramdinmawaii E. et. al., 2014).

III. CAUSES OF CYBERCRIME

i. Loss of evidence – Loss of evidence is a very general and common problem as all the data is frequently destroyed. For the collection of data outside the territorial extent also paralyzes the system of Cybercrime Investigation.

ii. Easy to Access – The problem encountered in guarding a computer system from unauthorized access is that there is every possibilities of breach not due to human error but due tocomplex technology. (Dashora K., 2011), By secretly implanted logic bomb, key loggers that can steal access code, advanced voice recorders, retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get pass many a security system.

iii. Capacity to store data in comparatively small space – The computer has a unique characteristics of storing data in a very small space. This allows for much easier access or removal of information through either physical or virtual media(Choudhury R. R. et. al., 2013).

iv. Negligence – Negligence is one of the characteristics in human conduct so there may be a possibly that secure and protecting the computer system we may make negligence which provides a Cyber-criminals the access and control over the computer system.

v. Complex – The computers works operating system and these operating system are programmed of millions of codes. The human mind is imperfect so, they can do many mistakes or errors at several stages.

III. (a) Laws of Cybercrime

All laws aren't the same in many countries especially when it comes to Cybercrimes. For different countries have specific laws governing problems such as Cybercrimes. For example, Insome countries such as India accepted The Information Act which was passed and enforces in 2000 on Electronic Commerce by the United Nations Commission on Trade Law. However, the act states that it will legalize e-commerce and supplementary modify the Indian Penal Code 1860, the act 1872, the Banker's Book Evidence Act 1891 and the Reserve Bank of India Act 1934.

The Information Technology Act deals with the various Cybercrimes. From this Act, The important sections are: Section 43,65,66,67. Section 43 which explain and enforces the unlawful access, transferring virus outbreaks causes harm for DOA. Section 67 of information Technology Act, 2000 deals with obscenity and pornographic content on internet.

III.(b)Cyber Laws in India:

Cyber Crimes, in India are registered under three main heads, The IT Act, The IPC (Indian Penal Code) and SLL (State Level Legislations) (https://www.jagranjosh.com/general knowledge/what-is-cyber-crime-and-how-it-is-increasing-day-by-day-1479450153-1).

Cases of Cyber Laws under IT Act:

- Tampering with computer source documents – Sec. 65
- Hacking with computer systems, Data alteration – Sec.66
- Publishing obscene information – Sec. 67
- Breach of Confidentiality and Privacy – Sec. 72
- Publishing false digital signature certificates – Sec.73

Cases of Cyber Laws under IPC and special Laws:

- Sending threatening messages by email – Sec. 404 IPC

- Email abuse – Sec.500 IPC
- Web-jacking – Sec.383 IPC
- Forgery of Electronic records – Sec 463 IPC
- Email spoofing – Sec.463 IPC
- Bogus websites, Cyber Frauds – Sec 420 IPC

Cyber Crime under special cells:

- Online sale of Arms Act
- Online sale of Drugs under Narcotic Drugs and Psychotropic Substances Act.

i. **Section 65-**Tempering with the computers source documents.

Whoever intentionally or knowingly destroy, conceal or change any computer's source code that is used for a computer, computer program and computer system or computer network (Sarmah A. et. al., 2017).

Punishment: Any person who involves in such crimes could be sentenced upto 3 years imprisonment or with a fine of Rs. 2 lakhs or with both.

ii. Section 66- Hacking with Computer system, data alteration etc.

Whoever with the purpose or intention to cause any loss, damage or to destroy, delete or to alter any information that resides in a public or any person's computer. Diminish its utility, values or affects it injuriously by any means, commits hacking(https://cybercrimelawyer.wordpress.com/category/information-technology-act-section-65/https:/cybercrimelawyer.wordpress.com/category/information-technology-act-section-65/).

Punishment: Any person who involves in such crimes could be sentenced upto 3 years imprisonment, or with a fine that may extend upto 2 lakhs rupees, or both.

iii. Section 66C- Identity theft

Using of one's digital or electronic signature or one's password or any other unique identification of any person is a crime.

Punishment: any person who involves in such crimes could be sentenced either with a description for a term which may extend upto 3 years of imprisonment along with a fine that may extend upto rupee 1 lakh.

Here are the some lists of Cybercrimes and Cyber Laws under the following section:

Table No.2

Cyber Attacks	Laws
Un-authorized access to protected system.	Section 70
Penalty for misrepresentation.	Section 71
Breach of confidentiality and privacy.	Section 72
Publishing false digital signature certificates.	Section 73
Publication for fraudulent purpose.	Section 74
Act to apply for contravention or offence that is committed outside India.	Section 75
Compensation, confiscation or penalties for not to interfere with other punishment.	Section 77
Compounding of Offences.	Section 77A
Offences by Companies.	Section 85
Sending threatening messages by e-mail.	Section 503 IPC
Sending defamatory messages by e-mail.	Section 499 IPC
Bogus websites, Cyber Frauds.	Section 420 IPC
E-mail Spoofing.	Section 463 IPC
E-mail Abuse.	Section 500 IPC
Criminal intimidation by anonymous communications.	Section 507 IPC
Online sale of Drugs.	NDPS Act
Online sale of Arms.	Arm Act

IV. PREVENTION OF CYBERCRIME

i. To prevent cyber stalking avoid disclosing any information pertaining to one self.

ii. Never send your credit card number to any site that is not secured, to guard against frauds.

iii. Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of photographs.

iv. It is better to use a security program that gives control over the cookies and send information back to the sites as leaving the cookies unguarded might prove fatal.

v. Use of firewalls may be beneficial.

vi. Always keep back up data's so that one may not suffer data loss in case of virus contamination.

vii. Use strong biometrics as a Password/locker.

viii. Secure your mobile device.

ix. Avoid suspicious E-mail.

x. Protect your identity online.

xi. Call the right person for help.

xii. Check your accounts and your credit reports regularly.

V. CONCLUSION

From this research paper it has been found that there are several ways and means through which an individual can enact crimes are an offense and are punishable by law (Ramdinmawaii E. et. al., 2014). In this paper we have discussed about the types of cybercrimes, laws of cybercrimes in India, the causes of cybercrimes and how to prevent or avoid cybercrimes. The solution to such crimes can't be simply based on the technology. These technologies can just be one such weapon to track and put a break to such activities to some extent. The way to overcome these crimes can broadly be classified into three categories: Cyber Laws (referred as Cyber laws), Education and policy making. All the above ways to handle cybercrimes either are having very less significant work or having in many of the countries. This lack of work requires to improve the existing work or to set new paradigms for controlling the cyber-attacks.

VI. REFERENCES

[1]. Choudhury R. R. et. al., (2013), Cyber Crimes-challenges and Solutions, International Journal of Computer Science and Information Technology, Volumes: 04, PP. 729-732.

[2]. Dashora K., (2011), Cyber Crime in the Cociety: Problems and Preventions, Journal of Alteranative Perspectives in the Social Sciences, Volume: 03, Issue: 01, PP. 240-259.

[3]. Ramdinmawaii E. et. al., (2014), A Study on Cyber-crime and Cyber Criminals: A Global problem, International Journal of Web Technology, Volume: 03, PP. 172-179.

[4]. Saini H. et. al., (2012), Cyber-Crimes and their Impacts: A Review, International Journal of Engineering Research and Applications, Volume: 02, Issues: 02 PP. 202-209.

[5]. Sarmah A. et. al., (2017), A study on Cyber-crime and Cyber Law's of India, International Research Journal of Engineering and Technology, Volume: 04 Issue: 06 PP. 1633-1640.

[6].https://www.jagranjosh.com/general-knowledge/what-is-cyber-crime-and-how-it-is-increasing-day-by-day-1479450153-1

[7].https://cybercrimelawyer.wordpress.com/category/information-technology-act-section-65/https:/cybercrimelawyer.wordpress.com/category/information-technology-act-section-65/