AN ANALYSIS ON CYBER CRIMES

***ANDUKURI ANOOP**

Historical Background:

Cyber crime is a crime which involves a computer or a network. From the very first cyber crime that has been committed in 1820, cyber threats have grown in scope and complexity. It is very difficult to believe that cybercrime work committed even before internet came into existence. But it is true that the first instances of cyber crime were data thefts.

The first cyber crime has been committed in the year 1820 by Jaquard. [1]Jaquard is a textile manufacturer in France and found a device which repeated a series of steps in weaving of special fabrics. [2]The employees who were afraid of losing their traditional employment committed acts of sabotage and discouraged Jacquard not to use this device thereby performing the world's first cyber crime. After that criminals regularly used to commit crimes via telephone lines.

The calls were disconnected and redirected so that they can be used for personal usage. Then slowly computers came into existence and along with that cybercrime also evolved in the 80s. People started to hack another persons computer and misuse the personal data and information in it. There is no single target for cyber crime, even though it started with telephone companies it slowly shifted it targets to banks web-shops and individuals. The people who commit cybercrime do it for different purposes. Some do it to earn money, some do it just for fun and others do it to give a public message.

[3]Now cybercrime has a lot of scope because we are very dependent on the computers in modern life. This includes financial crimes, sale of illegal articles, online gambling, intellectual property crimes, email spoofing, forgery, drug trafficking, cyber defamation, cyberstalking and so on.

---

[1] http://www.bezaspeaks.com/cybercrime/history.htm (last visited on 5th June)

[2] http://www.bezaspeaks.com/cybercrime/history.htm (last visited on 5th June)

[3]http://www.inf.tsu.ru/WebDesign/libra3.nsf/317094d25b4410c6c62571f5001deba4/3b47f7a6821452fdc62572040016d843/$FILE/cybercrime.(last visited on 3rd June)

Types of Cyber Crimes:

Malware: Malware is a contraction of malicious software into a system for the benefit of the third party without the permission of the user. Its generally a written software with the intention to create harm to the devices like phone, tablet and etc. It includes worms, Trojan horses, computer viruses and etc.

There are different types of Malware namely:

Trojan horse: It is a type of Malware which completely obtains control over once system and can steal sensitive data or it may turn the computer in such a way to carry out fraud. There are many types of Trojan such as backdoor, infostealer, mailfinder, remote access trojan, rootkit trojan and etc.

Spyware: It is a type of Malware which is installed in a device and gathers sensitive information without the knowlege of the user. It usually controls the entire device ,tracks the data usage, obtains sensitive information and credit card details. There are different types of Spyware namely adware, modem hijacker, browser hijacker and etc.

Logic Bombs: [4]Logic Bomb is a type of malware which uses trigger to activate the malicious code and causes harm to a computer.

Phishing: Phishing is a procedure of gathering information by sending fraudulent e-mails. The main aim of this Phishing attack is to grab details like credit/debit card details, usernames and passwords. This mainly started in mid 1990s and it is one of the oldest type of Cyber attack.

Cyberstalking: Cyberstalking is a crime which uses different electronic communications like emails, chat rooms, instant messaging and etc to harass an individual, group or an organization.

[4] comodo.com/blog/comodo-news/logic-bomb (last visited on 4th June)

Identity Theft: It is a type of Cyber crime which intentionally uses someone's identity to obtain personal or financial information for personal gain which results in loss to other person.

Internet fraud: It is a type of Cyber crime which uses the internet and involve hiding of information or taking advantage of them. This can be committed in many forms like e-mails that attempt to seek financial information and etc.

Important cases in Cyber Crimes:

SONY.SAMBANDH.COM CASE:

[5]Sony India Private Ltd. which runs a website called www.sony-sambandh.com and in May 2002, someone logged onto website under the identity of Barbara Campa and placed an order for Sony T.V and a cordless head phone. She gave her credit card details for the payment and requested to deliver the products to Arif Azim in Nodia. After that the company delivered the things to Arif Azim and took the photographs showing that the delivery being accepted by Arif Azim. But after one and a half month the credit card agency informed that this was an unauthorized transaction. Finally the company filed a complaint for online cheating at CBI (Central Bureau of Investigation) and registered the case under Section 418, 419, and 420 of IPC. The case was investigated and Arif Azim was arrested. It revealed that Azim was working at a call centre in Noida and had accessed the credit details and misused. The court of Shri Gulshan Kumar Metropolitan Magistrate, New Delhi convicted Arif Azim and further court felt that the accused was a young boy (24 years) and it was first time that cyber crime has been convicted. Therefore the court released the accused.

The Bank NSP Case:

In this case a management trainee was engaged to be married. The couple exchanged emails via company's computer. After that the couple broke up and the girl created fraudulent emails like " Indian bar associations" and sent to the boy's foreign clients. She used the company's computer for doing this and the boy's company lost many clients. Finally the bank was held liable for the mails sent via bank's computer.

[5]http://www.legalserviceindia.com/lawforum/cyber-laws/17/sony-sambandh-com-case-india-saw-its-first-cybercrime-conviction/2242/ (last visited on 1st June)

Suhas Katti v. Tamil Nadu: This is the first time where a conviction was handed down regarding with posting of obscene messages on internet. In this case a women , complained that a man was sending obscence messages. The police found that the accused was interested in marrying her but she was not interested in marrying him. The accused started harassing her through online. [6]On 5th November 2004 the magistrate found that the accused was guilty of offence under Section 469,509 of Indian Penal Code and 67 of IT Act 2000. [7]He was sentenced to RI for two years under Section 469 of IPC and a fine of rupees five hundred, one simple imprisonment and fine of rupees five hundred under Section 509 of IPC and two years imprisonment with fine of rupees four thousand under Section 67 of IT Act 2000.

Cyber laws in India:

The Information Technology Act 2000 was passed by Parliament of India to provide legal recognition for E- commerce and electronic transactions. It was again amended by passing The Information Technology (Amendment) Act 2008.

[8]Sections of the Act which deal with offences called as Cyber crimes.

- Section 65 of the IT Act deals with tampering with computer source documents. Punishment: imprisonment up to 3 yrs, or fine up to Rupees 2 lakh, or with both.
- Section 66 of the IT Act deals with hacking with the computer systems. Punishment: imprisonment for a term which may extend to 3 years, or fine up to Rupees 5 lakh, or with both. Section 66 has widened after ITAA.

  Section 66A deals with sending offensive messages through communication services etc. Punishment: imprisonment for a term which may extend to 3 yrs and with fine.

  Section 66B deals with dishonestly receiving stolen computer resource or communication device. Punishment: imprisonment of either description for a term which may extend up to 3yrs or with fine which may extend to Rs 1 lakh, or with both.

[6] https://en.wikipedia.org//wiki/Suhas_Katti_v._Tamil_Nadu (last visited on 3rd June)
[7] https://en.wikipedia.org//wiki/Suhas_Katti_v._Tamil_Nadu (last visited on 3rd June)
[8] https://www.tutorialspoint.com/information_security_cyber_law/information_technology_act.htm (last visited on 1st June)

Section 66C deals with punishment for identity theft. Punishment: imprisonment of either description for a term which may extend up to 3yrs and with fine which may extend to Rs 1 lakh

Section 66D deals with punishment for cheating by personation using computer resource. Punishment: imprisonment which may extend up to 3yrs and fine which may extend to 1 lakh.

Section 66E deals with punishment for violation of privacy. Punishment: imprisonment which may extend to three yrs, or with fine up to two lakh, or both.

Section 66F deals with cyber terrorism. Punishment: imprisonment which may extend to life imprisonment.

- Section 67 of the IT Act deals with publishing of obscene information in electronic form. Punishment: imprisonment of either description for a term which may extend to 3yrs and with fine which may extend to Rupees 5 lakh for first conviction and imprisonment of either description for a term which may extend to five years and fine which may extend to Rs 10 lakh on subsequent conviction.

  Section 67A deals with publishing of transmitting material. Punishment: imprisonment of either description for a term which may extend to 7 years and also with fine which may extend to 10 lakh rupees.

  Section 67B deals with publishing of transmitting material depicting children. Punishment: imprisonment of either description for a term which may extend to 7 years and also with fine which may extend to 10 lakh rupees.

  [9] Section 67C deals with preservation and retention of information by intermediaries. Punishment: imprisonment for a term which may extend to 3yrs and fine.
- Section 68 of the IT Act deals with power of controller to give directions. Punishment: imprisonment for a term not exceeding two years or fine not exceeding Rupees 1 lakh or both.
- Section 69 of the IT Act deals with Directions of Controller to a subscriber to extend facilities to decrypt information. Punishment: imprisonment for a term which may extend to seven years and fine.

[9] https://indiankanoon.org/doc/91763765/

- Section 70 of the IT Act deals with Protected system. [10] Punishment: imprisonment of either description for a term which may extend to 10 years and fine.
- Section 71 of the IT Act deals with Penalty for misrepresentation. Punishment: imprisonment for a term which may extend to 2 years, or with fine up to 1 lakh, or with both.
- Section 72 of the IT Act deals with Penalty for breach of confidentiality and privacy. Punishment: imprisonment for a term which may extend to two years, or fine up to rupees one lakh, or with both.

  Section 72A deals with disclosure of information in breach of lawful contract. Punishment: imprisonment up to three years or with fine up to five lakh rupees, or with both.
- Section 73 of the IT Act deals with penalty for publishing Digital Signature certificate false in certain particulars. Punishment: imprisonment for a term which may extend to two years, or with fine which may extend to rupees one lakh, or with both.
- Section 74 of the IT Act deals with publication for fraudulent purpose. Punishment: imprisonment for a term which may extend to two years, or
- with fine which may extend to rupees one lakh, or with both.

Conclusion:

In this digital world, the rate of cyber crimes are increasing day by day. As the new technology arrives the cyber crimes also increases. Life has become so comfortable in making online shopping's, transactions and etc. But the rate of cyber crime are not decreasing. According to me the laws relating to cyber crimes should be tightened and strictly implemented. Even the offences which are not included in Information Technology Act 2000 should be included.

[10] https://indiankanoon.org/doc/91763765/