International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838; Print ISSN: 2664-682X
Received: 02-01-2020; Accepted: 03-02-2020; Published: 03-03-2020
Volume 2; Issue 1; 2020; Page No. 15-19

Cyber Crimes in India

Neha Sharma
Student, Department of Criminology, MDC, Panchkula, Haryana, India

Abstract
This subject has become very popular in the society because Cyber Crime is associated with the people who are quite educated and who have sufficient knowledge about the information technology Cyber Crimes are a type of fraud, which requires knowledge and greater skill for accomplishing the task. Cybercriminals are using more advanced and scalable tools to breach user privacy, and they are getting results. Two billion data records compromised in 2017, and more than 4.5 billion records were breached in the first half of 2018 alone. Here are the most pressing cyber-security issues in 2019, as well as rising trends into 2020.

Keywords: cyber crime, technology, fraud, cybercriminals

Introduction
In today's world every person largely dependent upon the internet and use of technology, the incidents of Cyber Crime have increased. Cyber Laws in India prevent any crime done using technology, where a computer is a tool for cybercrime. The laws for Cyber Crime protect citizens from dispensing sensitive information to a stranger online. Ever since the introduction to cyber laws in India happened, IT Act 2000 enacted and amended in 2008 covering different types of crimes under cyber law in India. In a Cyber Crime, computer or the data itself on target or the object of offence or a tool in committing some other offences, providing the necessary inputs for that offenc [1]. Common internet users may be unaware of cybercrimes, let alone what to do if they fall victim of cyber-attacks. Many innocent individuals fall victim to cybercrimes around the world, especially since technology is evolving at a rapid pace. Cybercrimes are any crimes that cause harm to another individual using a computer and a network. Cybercrimes can occur by issues surrounding penetration of privacy and confidentiality. When privacy and confidential information is lost or interrupted by unlawfully individuals, it gives way to high profile crimes such as hacking, cyber terrorism, espionage, financial theft, copyright infringement, spamming, cyber warfare and many more crimes which occur across borders. Cybercrimes can happen to anyone once their information is breach by an unlawful user. The purpose of this paper is to educate individuals who don't know what are cybercrimes and its importance in growing technological advance throughout society. Understanding the threat of cybercrimes is a very pertinent issue because technology holds a great impact on our society as a whole. Cybercrime is growing every day because since technological advancing in computers makes it very easy for anyone to steal without physically harming anyone because lack of knowledge to the general public of how cybercrimes are committed and how they can protect themselves against such threats that cybercrimes poses. In 2017 Wannacry incident, in which a cyber-attack disabled the IT systems of many organisations including the NHS, demonstrates the real-life consequences that cyber-attacks can have.

These attacks are becoming increasingly sophisticated, using psychological manipulation as well as technology. Examples of this include phishing emails, some of which can be extremely convincing and credible. Such phishing emails have led to cyber-security breaches at even the largest of technology companies, including Facebook and Google.

To face these challenges, society needs cyber security professionals who can protect themselves from damages Yet the demand for qualified cyber security practitioners has quickly outpaced the supply, with three million unfilled cyber security posts worldwide [2].

Definition
Cyber Crime is not defined in Information Technology Act 2000 nor in the I.T. Amendment Act 2008 nor in any other legislation in India. Offence or crime has been dealt with elaborately listing various acts and the punishments for each, under the Indian Penal Code, 1860 and quite a few other legislations too. Hence, to define Cyber Crime, 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 Cyber Crime [3].

The law relating to Cyber Crime in India
The offences as hacking is violation of right of privacy as recognized a fundamental Rights by the Apex Court of India. However, considering the need of International Society and for giving effect to the UN resolution the Indian legal system requires the law relating to the computer and Internet therefore the Information Technology Act and certain special rules enacted by the Indian legal

[1] https://www.myadvo.in/blog/what-is-the-cyber-law-in-india/ (Visited on 29 June 2019)

[2] https://theconversation.com/theres-a-massive-cybersecurity-job-gap-we-should-fill-it-by-employing-hackers-114643 (visited on 29 june 2019)

[3] Ibid.

system. Due to certain technical nature, certain amendments also need therefore the

Indian Legal system formulated the rules to maintain its legal status in international family. Indian legal system enacted Information Technology Act, 2000 with intent to regulate the e-business. That is purely a contractual law dealing with the commerce, but along with e-business, it provides certain provisions dealing with unauthorized use of the internet or unauthorized use of the computer. This misuse is called as a Cyber Crime in The Information Technology Act, 2000, which is India's cyber Law. The offences provided in this Act are already provided in Indian Penal Code in the various provision from the enactment of the Indian Penal Code [4]. After coming into force of the Information Technology Act, 2000 on 17th October,2000 appropriate provisions have been incorporated in the substantive criminal law of India**.** It contains wide range of offences such as tempering with computer sources, sending offensive messages, violation of privacy; publishing obscene material etc. these all illegal activities are already recognized as an offence in Indian Penal Code. These similarities can discuss in the following ways; Similar offences also fall under the Indian Penal Code.

1. Sending threatening messages by email ----Section 503 IPC
2. Sending defamatory messages by email--- Section 499 IPC
3. Forgery of electronic records---------- Section 463 IPC
4. Bogus websites, cyber frauds ---------- Section 420 IPC
5. Email spoofing ----------Section 463 IPC
6. Web-jacking ----------Section 383 IPC
7. E-Mail Abuse ---------- Section 500 IPC
8. Online sale of Drugs ----------NDPS Act
9. Online sale of Arms ---------- Arms Act
10. Pornographic ---------- Section 292 IPC

In Criminal Procedure Code, after Section 198 A [5], Section 198 B has been inserted according to which, "No Court shall take cognizance of an offence punishable under Sections 417, 419 and 502 of the Indian Penal Code, except upon a complaint made by the person aggrieved by the offence". Moreover, in the Indian Penal Code the meaning of some words like "offences" and "computer resource" has been made more exhaustive which take color from the IT Act, 2000. It shows that India is successful in facing new challenges of IT. Many amendments have been made in the Copy Right Act on the argument that certain knowledge should be treated as private property and capable of 'Ownership'. Considering the requirement of society now, cyber law is providing a worth in administration of justice. Apart from the Information Technology Act and Indian Penal Code, there are certain laws and regulations, which deal with the Cyber Crime. Even certain civil laws are relevant in certain misuse in cyber space. They are as

following.

1. Common Law (governed by general principles of law)
2. The Bankers' Book Evidence Act, 1891
3. The Reserve Bank of India Act, 1934
4. The Information Technology (Amendment) Act, 2008 and 2009
5. The Information Technology (Removal of difficulties) Order, 2002
6. The Information Technology (Certifying Authorities) Rules, 2000
7. The Information Technology (Certifying Authorities) Regulations, 2001
8. The Information Technology (Securities Procedure) Rules, 2004
9. Various laws relating to IPRs.

Causes of Cybercrimes and Methods of Committing

Crime is a social phenomenon and there are various reason behind the crime. Criminologist had studied by giving different reason but the entire criminologist gives different reason. Cyber Crime is creation of the technology and the technology makes the life of human being easy, therefore every one attracted towards this technology without sufficient knowledge. This technology is having various special feature due to which is gives opportunity to the misuse the technology for commission of crime.

As Prof. H. L.A. Hart in his classic work entitled, "The concept of law" has stated that, human beings are valuable to unlawful acts which are crimes and therefore, rules of law are required to protect them against such acts. Applying the same analogy to cyber space, the computer systems despite being hi-tech devices are extremely vulnerable. This technology can easily be use to dupe or exploit a person or his computer by illegal or unauthorized access. The damage so caused to the victim may be direct or indirect result of abuse of computer systems. In the absence of any foolproof mechanism to protect and safeguard innocent computer users against cyber criminality, the cyber criminals indulge in criminal activities through networks unabated without any fear of being apprehend and tried for the offence committed by them. There are many ways or means where cybercrimes can occur. Here are a few causes and methods of how cybercrimes can be committed on a daily basis: Hacking, Theft of information contained in electronic form, Email bombing, Data diddling, Salami attacks, Denial of Service attack, Virus / worm attacks, Logic bombs, Trojan attacks, Internet time theft, and Web jacking [6].

- **Hacking*:*** In other words, can be referred to as the unauthorized access to any computer systems or network. This method can occur if computer hardware and software has any weaknesses which can be infiltrated if such hardware or software has a lack in patching, security control, configuration or poor password choice.
- **Theft of information contained in electronic form*:*** This type of method occur when information stored in computer systems are infiltrated and are altered or physically being seized via hard disks; removable storage media or other virtual medium.
- **Email bombing:** This is another form of internet misuse where individuals directs amass numbers of mail to the victim or an address in attempt to overflow the mailbox, which may be an individual or a company or even mail servers there by ultimately resulting into crashing. There are

[4] Laws on Cyber Crime: P.K.Singh (2007), Book Enclave, Jaipur, First Publication. Page 96.
[5] Section 198 A of Cr. P.C. 1973
[6] http://www.naavi.org/pati/pati_cybercrimes_dec03.htm (Visited on July 5, 2019)

two methods of perpetrating an email bomb which include mass mailing and list linking.

- **Data diddling*:*** Is the changing of data before or during an intrusion into the computer system. This kind of an occurrence involves moving raw data just before a computer can processes it and then altering it back after the processing completed.
- **Salami attacks:** This kind of crime is normally consisting of a number of smaller data security attacks together end resulting in one major attack. This method normally takes place in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed. This form of cybercrime is very common in banks where employees can steal small amount and it's very difficult to detect or trace an example is the "Ziegler case" where in a logic bomb penetrated the bank's system, which deducted only 10 cents from every account and deposited it in one particular account which is known as the "penny shaving".
- **Denial of Service attack:** Basically, where a computer system becomes unavailable to it is authorize end user. This form of attack generally relates to computer networks where the computer of the victim is submerged with more requests than it can handle which in turn causing the pc to crash. E.g. Amazon, Yahoo. Other incident occurs in November, 2010 whistle blower site wikileaks.org got a DDoS attack.
- **Virus / worm attacks***:* Viruses are programs that can embed themselves to any file. The program then copies itself and spreads to other computers on a network which they affect anything on them, either by changing or erasing it. However, worms are not like viruses, they do not need the host to attach themselves to but make useful copies of them and do this constantly till they consume up all the available space on a computer's memory. E.g. love bug virus, which affected at least 5 % of the computers around the world.
- **Logic bombs:** They are basically a set of instructions where can be secretly be execute into a program where if a particular condition is true can be carried out the end result usually ends with harmful effects. This suggests that these programs produced to do something only when a specific event (known as a trigger event) occurs. E.g. Chernobyl virus.
- **Trojan attacks:** The term suggests where a program or programs mask themselves as valuable tools but accomplish damaging tasks to the computer. These programs are unlawful which flaccidly gains control over another's system by assuming the role as an authorised program. The most common form of a Trojan is through e-mail. E.g. lady film director in the U.S.
- **Internet time thefts:** This form is kinds of embezzlement where the fraudulent uses the Internet surfing hours of the victim as their own which can be complete by obtaining access to the login ID and the password, an example is Colonel Bajwa [7] case- in this incident the Internet hours were used up by a unauthorized person.
- **Web jacking*:*** This is where the hacker obtains access and can control web site of another person, where he or she can destroy or alter the information on the siteas they see fit to them.This type of method of cybercrime is done for satisfying political agendas or for purely monetary means. An example of such method was MIT (Ministry of Information Technology) was hacked by the Pakistani hackers whereas another was the 'gold_fish' case, site was hacked and the information relating to gold fish was altered and the sum of $ 1 million was demanded [8].

Cybercrime and cyber security

Cybercrime and cyber security are issues that can hardly be separated in an interconnected environment. The fact that the 2010 UN General Assembly resolution on cyber security [9] addresses cybercrime as one major challenge underlines this. Cyber security plays an important role in the ongoing development of information technology, as well as Internet services. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being. At the national level, this is a shared responsibility requiring coordinated
action related to prevention, preparation, response and recovery from incidents on the part of government authorities, the private sector and citizens. At the regional and international level, this entails cooperation and coordination with relevant partners. The formulation and implementation of a national framework and strategy for cyber security thus requires a comprehensive approach.39 Cyber security strategies – for example, the development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime – can help to reduce the risk of cybercrime.40 The development and support of cyber security strategies are a vital element in the fight against cybercrime.41 The legal, technical and institutional challenges posed by the issue of cyber security are global and far reaching, and can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation.42 In this regard, the World Summit on the Information Society (WSIS)43 recognized the real and significant risks posed by inadequate cyber security and the proliferation of cybercrime. The development of adequate legislation and within this approach the development of a cybercrime related legal framework is an essential part of a cyber security strategy. This requires first of all the necessary substantive criminal law provisions to criminalize acts such as computer fraud, illegal access, data interference, copyright violations and child pornograph [10]. The fact that provisions exist in the criminal code that are applicable to similar acts committed outside the network does not mean that they
can be applied to acts committed over the Internet as well. Therefore, a thorough analysis of current national laws is vital to identify any possible gaps. Apart from substantive criminal law

[7] Col. S.S. Bajwa v. Union of India AIR 1999.
[8] http://www.naavi.org/pati/pati_cybercrimes_dec03.htm (visited on July 5, 2019)

[9] UNGA Resolution: Creation of a global culture of cyber security and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.
[10] *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, P.141.

Provisions, the law-enforcement agencies need the necessary tools and instruments to investigate cybercrime. Such investigations themselves present a number of challenges. Perpetrators can act from nearly any location in the world and take measures to mask their identity.56 The tools and instruments needed to investigate cybercrime can be quite different from those used to investigate ordinary crimes [11].

The cyber crime economy

Cybercrime has its own economy that takes place on the dark web, which is different from the deep web. Criminals buy and sell malware, botnets, data lists and more to commit fraud and identity theft. That said, there is a more sinister side to the dark web.

The dark web is used for sex trafficking, distribution of child pornography, hitmen and much more. There is a corner of the internet, hidden by multiple redirects and encrypted pages, that opens up those horrible crimes. We called it the "cybercrime economy."

Because of the long paper trail left behind by using the internet, anonymity is the primary concern for criminals taking part in those activities. A combination of Tor and a secure virtual private network, along with the trust of others who run in those circles, usually allows people to access relevant areas of the dark web.

Your information, especially if it has been part of a data breach, is likely on the dark web and available for purchase. In most cases, your identity used to make false purchases. On the internet, everyone can use a different name and face, though, so it's sometimes used to carry out additional crimes. Protecting your personal data is paramount, not only for the number in your bank account, but also for your freedom.

Ethical Hacking

It is important to stress here that hacking is not an inherently illegal activity. There are many opportunities to engage in ethical hacking, which refers to attempting to hack systems for the purpose of finding and fixing the flaws that malicious hackers may try to exploit for criminal activity.

Our research demonstrates that the majority of people active within hacking communities have no wish to exploit the flaws they find although they do believe that such flaws should be exposed so that they can be addressed especially when the organisation concerned is holding public data and have sufficient resources that it is reasonable to feel they should not have any gaps in their cyber security in the first place. Several large and well-known companies actively engage with this culture, by offering hackers "bug bounties" financial rewards for identifying and reporting previously undiscovered weaknesses in their systems.

Prevention and Procedure

There are some ways however to avoid becoming a victim of cybercrime. Most internet browsers email service, and Internet providers provide a spam-blocking feature to prevent unwanted messages, such as fraudulent emails and phishing emails, from getting to your inbox. However, every user must ensure to turn them on and do not turn them off whatsoever. Also, users must install and keep up-to-date antivirus programs, firewalls and spyware checkers. Along with keeping them up to date, users must make sure that they run the scans regularly. There are many companies out there that provide free software, but there are other you can purchase, along with that of the many produced by the leading companies' providers; in addition, those companies provide free version of their paid or subscription antivirus software. Encryption of information that you do not want anyone to have unauthorized access to is a good way to avoid some cybercrimes; information such as password and credit card information for example. Encryption software runs your data through encryption algorithms to make it unintelligible to anyone who tries to hack into your computer.

Another good precaution is to be weary of who you divulge your personal information to. Try to avoid unknown websites, in particular those that ask for your name, mailing address, bank account number or social security number. When doing online shopping make sure website is secure, look for urls that starts with "https" and/or have the Trustee or VeriSign seal. If you do not see these anywhere on the site, you run the risk of submitting credit card information and other personal information to a site that maybe a fraud.

Another way to avoid being a victim of cybercrimes is to avoid being susceptible to common frauds, such as inherences letter, letter asking for your help in placing large sums of money in overseas bank accounts, foreign lotteries, and phony sweepstakes. Those mentioned activities are all methods used by cyber criminals to get your personal information and money. If it sounds too good to be true, it probably is.

Educate children about the proper use of the computer and internet and make sure to monitor their online activities at home and school alike. They should only have access to a computer located in a central area of your home and you should regularly check all browser and email activity. A wise thing to is to use parental control software that limits the type of sites the user can gain access to. In schools, there should be restricted websites and other user restrictions that will help protect the user and entity from cybercrime. Likewise, companies should educate and have written policies governing the workplace pc and its network use to diminish the risk of cybercrime against the company.

One definite way to ensure that you do not fall victim of cybercrimes is to disconnect your computer entirely from the internet. If there is no network, then you don't have to worry about any cyber-attacks. However, this option is not the most viable one in our interconnected society. The truth is, it is up to you to take the necessary precautions to avoid potential cybercrimes.

Conclusion

Computer users and internet connectivity is growing very fast in India. So it will be a very hard task to curb and control Cyber Crime. India has to make its I.T. Act (2000) more comprehensive to cover all fields of Cyber Crime and ensure stringent enforcement to the highest level. Besides, the common public and computer users should be made aware and conscious of various types of Cyber Crimes. Capacity of human mind is unfathomable. It is not possible to eliminate Cyber Crime from the cyber space. However, it is quite possible to check them. Users must try and save any electronic information trail on their computers, use of

[11] Ibid.

anti-virus software, firewalls, use of intrusion detection system etc. and further making the application of the laws more stringent to check crime.

References

1. https://www.myadvo.in/blog/what-is-the-cyber-law-in-india/ Visited on 29 June, 2019.
2. https://theconversation.com/theres-a-massive-cybersecurity-job-gap-we-should-fill-it-by-employing-hackers-114643 visited on 29 june, 2019.
3. Ibid.
4. Laws on Cyber Crime: P.K. Singh, Book Enclave, Jaipur, First Publication, 2007, Page 96.
5. Section 198 A of Cr. P.C, 1973.
6. http://www.naavi.org/pati/pati_cybercrimes_dec03.htm Visited on July 5, 2019.
7. Col SS, Bajwa V. Union of India AIR, 1999.
8. http://www.naavi.org/pati/pati_cybercrimes_dec03.htm visited on July 5, 2019.
9. UNGA. Resolution: Creation of a global culture of cyber security and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.
10. Gercke, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 141.
11. Ibid.