IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

ANALYZE THE COST OF CYBER CRIME AND DIGITAL SPYING

R. Janani
Assistant professor
Govt law college, Madurai.

ABSTRACT

The world today is experiencing an exponential growth in cyberspace. Nevertheless, India too has witnessed a significant ascend in Internet activities and it is quite assertive to say that such phenomenal growth in access to information on one hand leads to empowered individuals and organization and on the other hand also poses new challenges to government and citizens. Cybercrime is a crime that involves a computer and a network. The computer may have been used to commit the crime and in many cases, it is also the target. Cybercrime may threaten a person or a nation's security and financial health. the prime objective of the government is to prevent cyber-attacks and to protect the country's critical infrastructure. It also focuses on reducing vulnerability to cyber-attacks so as to reduce and minimize damage and recovery time. To prevent the cybercrimes, individuals and governments need to clearly understand the crime schemes in the cyberspace and the contemporary and continuing Internet trends and behaviors of these criminals. Cybercrime is estimated to cost the world $10.5 trillion annually by 2025. Cybercrime costs make up a value worth 1% of the Global GDP.The average cost of a ransomware attack went down slightly, from USD 4.62 million in 2021 to USD 4.54 million in 2022. The average ransomware cost of $4.54 million is slightly higher than the overall average total cost of a data breach, USD 4.35 million.

Key words; cyber crime,Internet,Computer

1.INTRODUCTION

Cybercrime is a term that covers a broad scope of criminal activities by means of a computer. Cybercrime is referred to the act of performing criminal act using cyberspace as the communication medium. The cybercrimes like cyber bullying and cyber defamation are common issues and are rapidly increasing. The government is

framing policies and laws to prevent the growing number of such crimes. Most of the countries are not fully equipped with the legal infrastructure to handle cybercrimes. Young children and youth are among the most targeted section of the society that is affected by the perilous effects of electronic media. These activities are such as computer related frauds, cyber defamation, cyber harassment, child predation, identity theft, extortion, travel scam, stock market manipulation, complex corporate espionage, planning or carrying out terrorist activities, health care, insurance/bonds frauds, auction frauds, fake escrow scams, blackmail, non-delivery of merchandize, newsgroup scams, credit card frauds, email spoofing etc. Cybercrimes are committed using computers and computer networks. They can be targeting individuals, business groups, or even Government.

2. LITERATURE REVIEW

Nappinai N. S. (2010)

The author in his paper "Cyber Crime Law in India has law kept pace with Emerging Trends? An Empirical Study" highlighted some important provision of the criminal laws in India relating to data protection, privacy, encryption and other cybercrime activities and to the extent said provisions are enforced to fight not just the present but future trends in Cyber Crime.

Shrikant A. et al. (2010)

This paper deals with the privacy issue in Indian perspective with respect to challenges in three different dimensions like Legal, Technical and Political domain. Authors discuss about proposed framework to deal with these challenges. In India there is no such legal framework to deal with privacy issue. To handle major challenges, we refer ITA 2003 that was built with the motivation to facilitate e commerce and hence the privacy was not the prior concern in IT act. This paper provides a solution as per present and future requirement of privacy in Indian Scenario.

Ashwini B. (2012)

Author discusses broadly about the ratio of increasing cybercrime and their effect on the society and e business and retailers. The paper briefs about the cyber threat and frauds, it also briefs about the internet user in India, its scope and future. Author also puts light on the governmental measures to stop cybercrime and talks about the challenges that India needs to face to beat cyber threat. Susheel B. and Durgesh P. (2011)

Authors in their paper "Study of Indian Banks Websites for Cyber Crime Safety Mechanism" discusses that security plays an important role in implementation of technology specially in banking sector. Paper talks about the cyber security required at the core banking level as the money is just only single click away. Through this paper authors have tried to put forward different issues that Indian banking system face and importance of cyber security mechanism.

Sanjay P. (2010)

Author discusses in detail the provisions of IT Act, 2000 and its recent amendments towards combating cybercrime. Author has also made an attempt to analyze the current trends in cybercrime then the analyses is made on the needs of legislation and current provisions of IT Act, lastly paper talks about similar provisions in the world and drawing parallel laws in the country. Finally author sums up the discussion with suggested recommendations for possible and safe cyber world.

3.DEFINITION OF CYBER CRIME

The Indian Legislature doesn't provide the exact definition of Cybercrime in any statute, even the Information Technology Act, 2000; which deals with cybercrime doesn't define the term of cybercrime. In general the term cybercrime means any illegal activity which is carried over or with the help of internet or computers.

The oxford Dictionary defined the term cybercrime as "Criminal activities carried out by means of computers or the Internet." [1]

Dr. Debarati Halder and Dr. K. Jaishankar define cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones.[2]

"Cybercrime means any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them".[3]

Professor S.T. Viswanathan has given three definitions in his book The Indian Cyber Laws with Cyber Glossary is as follows –

1.Any illegal action in which a computer is the tool or object of the crime.

2. Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made a gain.

3. Computer abuse is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and transmission of data.[4]

4.CHARACTERISTICS OF CYBER CRIME

The Concept of cybercrime is very different from the traditional crime. Also due to the growth of Internet Technology, this crime has gained serious and unfettered attention as compared to the traditional crime.

1.People with specialized knowledge –

Cybercrimes can only be committed through the technology, thus to commit this kind of crime one has to be very skilled in internet and computers and internet to commit such a crime. The people who have committed cybercrime are well educated and have deep understanding of the usability of internet, and that's made work of police machinery very difficult to tackle the perpetrators of cybercrime.

2.Geographical challenges –

In cyberspace the geographical boundaries reduced to zero. A cybercriminal in no time sitting in any part of the world commit crime in other corner of world. For example, a hacker sitting in India hack in the system placed in United States.

3.Virtual World

The act of cybercrime takes place in the cyber space and the criminal who is committing this act is physically outside the cyber space. Every activity of the criminal while committing that crime is done over the virtual world

4. Collection of Evidence –

It is very difficult to collect evidence of cybercrime and prove them in court of law due to the nature of cybercrime. The criminal in cybercrime invokes jurisdiction of several countries while committing the cybercrime and at the same time he is sitting some place safe where he is not traceable.

5. Magnitude of crime unimaginable-

The cybercrime has the potential of causing injury and loss of life to an extent which cannot be imagined. The offences like cyber terrorism, cyber pornography etc. has wide reach and it can destroy the websites, steal data of the companies in no time.

5.CYBER SPYING

Cyber spying is the act or practice of obtaining secrets and information without the permission and knowledge of the holder of the information from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks or individual computers through the use of proxy servers.[5]

Cyber spying typically involves the use of such access to secrets and classified information or control of individual computers or whole networks for a strategic advantage and for psychological, political and physical subversion activities and sabotage. Cyber espionage attacks can result in damaged reputations and stolen data, including personal and private information. Cyber-attacks targeted at the government may cause military operations to fail, and can also result in lives lost due to leaked classified information. Cyber espionage is primarily used as a means to gather sensitive or classified data, trade secrets or other forms of IP that can be used by the aggressor to create a competitive advantage or sold for financial gain. In some cases, the breach is simply

intended to cause reputational harm to the victim by exposing private information or questionable business practices.

Cyber espionage attacks can be motivated by monetary gain; they may also be deployed in conjunction with military operations or as an act of cyber terrorism or cyber warfare. The impact of cyber espionage, particularly when it is part of a broader military or political campaign, can lead to disruption of public services and infrastructure, as well as loss of life.

The Supreme Court on Wednesday said indiscriminate spying on individuals cannot be allowed in a democratic country, governed by the rule of law, except with sufficient statutory safeguards, as such surveillance, either by the state or by any external agency, directly infringed upon the right to privacy.[6]

6.CYBER LAWS IN INDIA

INFORMATION TECHNOLOGY ACT,2000

The Information Technology Act, which came into effect in 2000, regulates cyber laws in India. The main goal of this Act is to safeguard eCommerce's legal protection by making it simple to register real-time records with the government. The sophistication of cybercriminals and people's propensity to abuse technology led to a number of adjustments.

section 10A

The effect that contracts concluded electronically shall not be deemed to be unenforceable solely on the ground that electronic form or means was used.

section 43A

To protect sensitive personal data or information possessed, dealt or handled by a body corporate in a computer resource which such body corporate owns, controls or operates. If such body corporate is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, it shall be liable to pay damages by way of compensation to the person so affected.

Sections 66A to 66F has been added to Section 66 prescribing punishment for offences such as obscene electronic message transmissions, identity theft, cheating by impersonation using computer resource, violation of privacy and cyber terrorism.

Section 67 of the IT Act, 2000 has been amended to reduce the term of imprisonment for publishing or transmitting obscene material in electronic form to three years from five years and increase the fine thereof from Rs.100,000 to Rs. 500,000. Sections 67A to 67C have also been inserted. While Sections 67A and B deals with penal provisions in respect of offences of publishing or transmitting of material containing sexually explicit act and child pornography in electronic form, Section 67C deals with the obligation of an intermediary to preserve and retain such information as may be specified for such duration and in such manner and format as the central government may prescribe.

The new amendments include an amended section 69 giving power to the state to issue directions for interception or monitoring of decryption of any information through any computer resource. Further, sections 69A and B, two new sections, grant power to the state to issue directions for blocking for public access of any information through any computer resource and to authorize to monitor and collect traffic data or information through any computer resource for cyber security.

Section 79 of the Act which exempted intermediaries has been modified to the effect that an intermediary shall not be liable for any third party information data or communication link made available or hosted by him if; (a) The function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; (b) The intermediary does not initiate the transmission or select the receiver of the transmission and select or modify the information contained in the transmission; (c) The intermediary observes due diligence while discharging his duties. However, section 79 will not apply to an intermediary if the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act or upon receiving actual knowledge or on being notified that any information, data or communication link residing in or connected to a computer resource controlled by it is being used to commit an unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

INDIAN PENAL CODE

Section 354c of IPC The cybercrime dealt with under this provision is capturing or publication of a picture of private parts or acts of a woman without such person's consent. This section exclusively deals with the crime of 'voyeurism' which also recognizes watching such acts of a woman as a crime. If the essentials of this Section (such as gender) are not satisfied, Section 292 of IPC and Section 66E of IT Act, 2000 is broad enough to take the offenses of a similar kind into consideration. The punishment includes 1 to 3 years of imprisonment for first-time offenders and 3 to 7 years for second-time offenders.

Section 354D of IPC: This section describes and punishes 'stalking' including both physical and cyberstalking. If the woman is being monitored through electronic communication, internet, or email or is being bothered by a

person to interact or contact despite her disinterest, it amounts to cyber-stalking. The latter part of the Section states the punishment for this offense as imprisonment extending up to 3 years for the first time and 5 years for the second time along with a fine imposed in both the instances.

In the case of Kalandi Charan Lenka v. The State of Odisha, ix the victim received certain obscene messages from an unknown number which are damaging her character. Moreover, emails were sent and the fake Facebook account was created by the accused which contained morphed pictures of the victim. Hence, the accused was found prima facie guilty for cyberstalking by the High Court under various provisions of IT Act and Section 354D of IPC

Section 379 of IPC: If a mobile phone, the data from that mobile or the computer hardware is stolen, Section 379 comes into the picture and the punishment for such crime can go up to 3 years of imprisonment or fine or both. But the attention must be given to the fact that these provisions cannot be applied in case the special law i.e IT Act, 2000 provisions are attracted.

In the case of Gagan Harsh Sharma v. The State of Maharashtra, x one of the employers found that the software and data were stolen and someone has breached the computers and gave access to sensitive information to the employees. The employer gave information to the police and they filed a case under Section 379, 408, and Section 420 of IPC and various other IT Act provisions. The question in front of the court is whether the police can file a case under IPC or not. The court decided that the case cannot be filed based on the IPC provisions as the IT Act has an overriding effect.

Section 411 of IPC: This deals with a crime that follows the offenses committed and punished under Section 379. If anyone receives a stolen mobile phone, computer, or data from the same, they will be punished in accordance with Section 411 of IPC. It is not necessary that the thief must possess the material. Even if it is held by a third party knowing it to be others, this provision will be attracted. The punishment can be imposed in the form of imprisonment which can be extended up to 3 years or fine or both.

Section 419 and Section 420 of IPC: These are related provisions as they deal with frauds. The crimes of password theft for the purpose of meeting fraudulent objectives or the creation of bogus websites and commission of cyber frauds are certain crimes that are extensively dealt with by these two sections of IPC. On the other hand, email phishing by assuming someone's identity demanding password is exclusively concerned with Section 419 of IPC. The punishments under these provisions are different based upon the gravity of the committed cybercrime.

CONCLUSION

The Information Technology Act is the sole savior to combat cybercrime in nature. Though offences where computer is either tool or target also falls under the Indian Penal Code and other legislation of the Nation, but this Act is a special act to tackle the problem of Cyber Crime. As we already know for a fact that the IT Act, 2000 has an overriding effect over the IPC provisions while governing the cybercrimes, there are a lot of instances where IPC provisions are applied based on the subjective circumstances of every case. Most of the countries are not fully equipped with the legal infrastructure to handle cybercrimes. Young children and youth are among the most targeted section of the society that is affected by the perilous effects of electronic media.

References

1.http://www.oxforddictionaries.com/definition/english/cybercrime (Accessed on 4th January, 2016)
2.http://www.naavi.org/pati/pati_cybercrimes_dec03.htm (Accessed on 4th January, 2016)
3.http://cybercrime.org.za/definition (Accessed on 4th January, 2016)
4. S.T. Viswanathan, The Indian Cyber Laws with Cyber Glossary, 2001, p. 81
5.http://www.indiancybersecurity.com/case_studies/state_of_tamil_nadu_%20suhas_katti.htm l (Accessed on 8th February, 2016)
6. https://www.deccanherald.com/national/indiscriminate-spying-on-individuals-cannot-be-allowed-supreme-court-1044762.html