International Journal of Advanced Research and Development
ISSN: 2455-4030; Impact Factor: RJIF 5.24
Received: 06-06-2019; Accepted: 08-07-2019
www.advancedjournal.com
Volume 4; Issue 5; September 2019; Page No. 42-44

Rapid increase of Cyber Crimes: A wake-up call for the law enforcement agencies

Kshamendra Mathur
Research Scholar, Department of Law, JNV University, Jodhpur, Rajasthan, India

Abstract
Technological breakthroughs in the Cyber landscape over the past few years have caused disruptions of immense magnitude with far reaching implications. On one hand, these have been enablers for good governance, smart policing, better medical care, etc., while on the other, there has been a surge in Cyber Crimes, frauds and data thefts. Frequent criminalization instances of the web have resulted in proliferation of various Cyber Crime. The protagonists have graduated from being opportunistic individuals to organized criminal groups who offer Cyber Crime service at a minimal cost over the dark net. To confront these new age Cyber criminals, a well thought and effective Cyber Crimes management strategy needs to be devised. If the Law Enforcement agencies have to win this battle, there is a need for a paradigm shift in the approach to policing. Therefore, in the current research paper a systematic understanding of increase of Cyber Crimes and why should Law Enforcement Agencies should concern about it are explained.

Keywords: law enforcement agency, cyber crimes

Introduction

Rapid and uncontrolled digitization coupled with inadequate response mechanism allows criminals to unleash Cyber Crimes through use of sophisticated tools which hide their identity and tamper, hinder or misdirect investigations. On the other hand, the law-enforcement agencies are still trying to upgrade their technical abilities to match the skills of their adversaries. With the ever-evolving threat landscape in the digital space, there is a constant need to upgrade technical proficiency and skills of the officers of Law Enforcement Agencies. Whilst most of these officers are well versed in basic Cyber Crimes investigation techniques, very few of them can be called Cyber Crimes specialists. Moreover, domain specialization is not institutionalized which further restricts their capability to monitor and check any form of Cyber Crimes including trading on the dark net, human trafficking, child and women sexual abuse material, digital forensics, Cyber frauds, etc.

Cyber Crime now costs the world almost $600 billion per year, or 0.8 percent of global GDP, which put global losses at close to $500 billion, or 0.7% of global income [1]. With global Cyber Crime damages predicted to cost up to $6 trillion annually by 2021, not getting caught in the landslide is a matter of taking in the right information and acting on it quickly [2].

India has witnessed a 457% rise in Cyber Crime incidents under the Information Technology (IT) Act, 2000 from the year 2011 to 2016, a recent The Associated Chambers of Commerce of India (ASSOCHAM-NEC) joint study said [3]. Symantec Corp ranked India among top five countries to be affected by Cyber Crime, between 2012-17, the number of internet users grew at the Compound Annual Growth Rate (CAGR) of 44%, of which India is placed third after US and China [4].

Out of the top 10 most targeted countries by Cyber attackers, India ranks fourth and Cybersecurity defenders are facing a lot of threats from these Cyber criminals. Cyber-attacks are an illegal activity and is continuously increasing in India for financial loot.

Cyber Attack is an attempt to destroy or infect computer networks in order to extract or extort money or for other malicious intentions such as procuring necessary information. Cyber-attacks alter computer code, data or logic via malicious code resulting in troublesome consequences which can compromise the information or data of the organizations to make it available to Cybercriminals. Cyber-attacks consist of various attacks which are hacking, D.O.S, Virus Dissemination, Credit Card Fraud, Phishing or Cyber Stalking [5].

Over the last few years, Cyber Crimes have become more intense, sophisticated and potentially debilitating for individuals, organizations and nations. Law Enforcement agencies are finding it difficult to check and prevent the crimes in the Cyber space because the perpetrators of these crimes are faceless and incur very low cost to execute a Cyber Crimes whereas the cost of prevention is extremely high. Targets have increased exponentially due to the increasing reliance of people on the internet. Cyber Crimes which were restricted to computer hacking till some time ago, have diversified into data theft, ransom ware, child pornography, attacks on Critical Information Infrastructure and so on. India is becoming increasingly vulnerable to this menace because of rapid digitization and proliferation of mobile data without matching pace of Cyber security and Cyber hygiene. At present, India is ranked third in terms of Cyber Crime incidents behind the United States and China as per data shared by a leading security vendor, which compiled data of bot-infected systems controlled by Cyber

criminals in different countries. As per Computer Emergency Response Team -India (CERT-IN), one Cyber Crime was reported every 10 minutes [6] in India during 2017. These statistics are quite alarming and therefore, merit focused and collective attention from Law Enforcement Agencies (LEA's).

Given the advantages of digital crime over its analog counterparts and the growing number of literate thieves, it is undoubtedly in the interest of Police and Law Enforcements agencies to learn as much as possible about Cyber Crime now, while there still remains a possibility of catching up with these criminals. The trends in Cyber Crime grow more alarming each year.

India ranks 3rd in terms of the highest number of internet users in the world after USA and China, the number has grown 6-fold between 2012-2017 with a compound annual growth rate of 44%. India secures a spot amongst the top 10 spam-sending countries in the world alongside USA. India was ranked among the top five countries to be affected by Cyber Crime, according to a 22 October report by online security firm" Symantec Corp [7].

The Internet has a global face. India, too, being a formidable part of the globe, felt a seismic shift in the technological setup when the Information Technology (IT) waves surged ahead and necessitated the formation of the IT ministry in the country in the year 1999. India was catching up with legal response to on-line activity and infraction when it came up with its first Cyber legislation, namely the IT Act, 2000. The Act has been amended in the 2008, enforced in the 2009 and has responded well to the means of Cyber Crime in the country. To protect the Critical Information Infrastructure (CII), a new agency namely, the Indian Computer Emergency Response Team (ICERT) is formed to respond to computer incident in the country [8]. Earlier in the 2003 CERT was formed to issue instructions in the context of blocking websites [9].

The crime graph of the country show that Cyber Security at stake. India is responding immensely to the communication revolution in the world and has legal equippers though at a rudimentary stage. While it is heading towards the goal of Global IT Super power, it is also fighting the means of Cyber Crimes. The IT Action Plan of the Government of India is striving towards making India the forerunner in the new technological age. It is aiming towards making India a "knowledge-based society [10]. Thus, the more technological savvy the country becomes, the lesser will be the chance of its exploitation by the online pirates through dense connectivity has its own blues and Cyber infraction are emerging as a challenge.

An analysis of the recent statistic of the Cyber Crime cases in India depicts the following results

a. Maximum number of cases under cyber-crimes were reported in Uttar Pradesh (2,639 cases) (21.4%) followed by Maharashtra (2,380 cases) (19.3%) and Karnataka (1,101 cases) (8.9%) during 2016.
b. During 2016, 48.6% of cyber-crime cases reported were for illegal gain (5,987 out of 12,317 cases) followed by revenge with 8.6% (1,056 cases) and insult to the modesty of women with 5.6% (686 cases) [11].
c. States which are mainly tribal like Sikkim, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Manipur, Meghalaya and some other state like Dadar and Nagar Haveli, Puducherry, Andaman and Nicobar island, Jammu and Kashmir show that there are least number of Cyber Crime reporting.
d. States Like Andhra Pradesh, Karnataka, Madhya Pradesh, Maharastra, Kerala and Punjab show increase in Cyber Crime reporting.
e. Strangely enough in Delhi, there is huge down fall in Cyber Crime cases, only 98 cases in year 2016 as compared to 177 cases in 2015 and 226 cases in 2014.
f. As on all India basis, number of Cyber Crimes has increased from 11592 in 2014 to 12317 in 2016 (Table) showing an increase of 5.88 per cent [12].
g. State of Uttar Pradesh, Mahrastra and Karnataka are on first, second and third position respectively in Cyber Crime cases in years 2016 whereas Rajasthan is at fourth position with slight decrease of 08% of cases in 2016 as compared to 2015.
h. In the 2016 total number of cases which were reported exclusively under IT Act was 16783 whereas only in 2710 cases charge sheets were submitted by Police [13].

To sum-up, in India, from 2014-2016, the Cyber fraternity has seen an increase in the number of perpetrators and there has been a constant rise in Cyber Crime incidents. Everywhere, the Cyber Crime regulatory regime is expanding its horizons through with little success so is it right to ask "….are we experiencing a calculated attempt to peddle Fear, Uncertainty and Doubt by the Cyber security industry – which has been described as a self-dramatizing and fear-mongering world of security pundits [14].

In Rajasthan Cyber Crimes are rapidly increasing due to extensive use of Internet and IT enabled services. The IT Act, 2000 specifies the acts which are punishable. Since the primary objective of this Act is to create an enabling environment for commercial use of IT, certain omission and commissions of criminals while using computers have been included in 2008 in the amended Act. Several offences having bearing on Cyber arena are also registered under the appropriate Section of the Indian Penal Code, 1860 (IPC) with the legal recognition of electronic records and the amendments made in several sections of the IPC vide the IT Act, 2000.

Information Technology has penetrated deep into the lives of citizens across the country and Rajasthan is no exception to it. As a corollary, crimes related to Information Technology have also increased in the State. Keeping in mind the challenges in handling Cyber Crimes faced in the State, Government of Rajasthan established a state-level Cyber Crime Police Station in State Crime Record Bureau through Gazette Notification No. F27 (ka) (7) Home-2/2011.

A total 938 cases of Cyber Crime have been registered in Rajasthan during the year 2016 as against 974 cases during 2015 which shows a decrease of 3.70%. The two metropolitan cities Jaipur and Jodhpur, the cases which were registered are as Jaipur City West registered the highest number of 203 cases under this head followed by Jaipur City South (138), Jaipur Rural (41), Jodhpur City West (36), Jodhpur City East (27). A total 175 persons were arrested in the year 2016 which shows a decrease of 11.17 percent as compared to 197 arrest in the year 2015. The highest number of 45 persons were arrested in Ajmer followed by Kota City 15 persons.

Conclusion

India is witnessing sharp rise in Cyber Crimes. Recently

released National Crime Record Bureau data show that there is continuous growth in Cyber Crimes. And so many persons were arrested for crimes that included hacking and obscene transmission, among others. Malware, spam, and phishing incidents are also rising. According to a survey report, India has overtaken the United States in spamming, which is a major source of malware distribution and creation of botnets. These, in turn, are used to launch many types of Cyber Crimes. Globally also, Cyber Crimes are rapidly increasing, since the financial payoffs are disproportionately high in comparison to efforts of criminals. United States estimates that it lost over USD one trillion in intellectual property in Cyber-attacks.

Handling Cyber Crimes requires an appropriate legal regime, technical infrastructure to analyse Cyber forensics data, and a trained Police workforce and prosecutors having knowledge of Cyber forensics tools for capturing evidence from the scene of crime and related network points, which can be anywhere in the country or in different parts of the world. Judiciary also has to be exposed to these concepts so that it can appreciate Cyber forensic evidence to make informed judgments. Capacity building of law-enforcement agencies is, therefore, a key element in bringing Cyber criminals to justice.

Cyberspace comprises IT networks, computer resources, and all the fixed and mobile devices connected to the global Internet. The size of Cyberspace continues to grow with increased Internet penetration, and activities that are carried through it including, the exchange of goods or services, financial transactions through banks, credit card payments, email communications, social networking, exchange of pictures, videos or music. The same networks are, however, used by criminals, by exploiting vulnerabilities in various devices, to commit Cyber Crimes that impact the physical world too. Cyber criminals carry out identity theft and financial fraud, steal corporate information, including intellectual property, conduct espionage to steal state and military secrets, and recruit criminals and others to carry out physical terrorist activities in the world. Cyber-attacks are also used to disrupt critical infrastructures such as financial and air traffic control systems, producing effects that are similar to terrorist attacks in physical space.

This study is a wake-up call to State and local Police to get in the field. Crime is changing, and Policing must change too. While overall Cyber Crime in the India is increasing. Local and State Governments must recognize that the crime fighting successes of these past so many years are not preparing us for the new crimes of this millennium.

References

1. Centre for Strategic and International Studies (CSIS) and McAfee. report, “The Economic Impact of Cybercrime: No Slowing Down”
2. https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/
3. https://telecom.economictimes.indiatimes.com/news/india-saw-457-rise-in cybercrime-in-five-years-study/67455224
4. https://telecom.economictimes.indiatimes.com/news/india-ranks-fourth-in-online-security-breaches/58411340
5. https://www.testbytes.net/blog/cyber-attacks-on-india-2018/
6. https://timesofindia.indiatimes.com/india/one-cybercrime-in-india-every-10-minutes/articleshow/59707605.cms
7. Presentation on Cyber Security by Dr. V.K. Saraswat, Member NITI Aayog.
8. S. 70-A and 70-B inserted by the IT (Amendment) Act, 2008 (10 of 2009)
9. Noticing the Increase in the number of Cyber Crimes in India, the Government of India issued notification by virtue of S.67 and 88 of the IT Act to constitute a Computer Emergency Response Team-India (CERT-IND). After receiving complaint, CERT-IND is to verify the authenticity of the complaint made and if considering it essential, CERT-IND shall instruct the Department of Telecommunications erring it essential, CERT-IND shall instruct the Department of Telecommunications (DoT)-KLR Cell to block the website. The DoT then checks as to when ISPs are working and then shall ensure blocking and informing CERT-IND accordingly.
10. Source: Introduction, Information Technology Action Plan, Government of India, 04.07.1998
11. Crimes in India 2016 Statics, Published by National Crime Records Bureau (Ministry of Home Affairs) Government of India.
12. Crimes in India 2016, National Crime Record Bureau, Chapter 18 “Cyber Crimes Ministry of Home Affairs.
13. Ibid
14. Wall DS. Cybercrime: The Transformation of Crime in the Information Age (University of Leeds, UK, 2007, 9.