Global Journal of Enterprise Information System

Emerging Trends in Cyber-Crimes

Devika Singh[1*]

[1*]LLB, Vivekananda institute of professional studies, I.P. University, Dwarka, Delhi, India; devikaddtlucans@gmail.com

Abstract

Unless and until our society recognizes cyber bullying for what it is, the suffering of thousands of silent victims will continue. 1Cyber crime is the most concerning issue for all countries, because it harms governmental confidential data as well as people in daily life transactions.Lack of proper training and education, the low level of awareness of the Indian society about the cybercrime has resulted into a spurt of cybercrimes. At times, even the law enforcement officers do not have proper training and other requisite expertise for tackling cybercrime. There are a huge number of cyber threats and their behavior is difficult to early understanding hence difficult to restrict in the early phases of the cyber attacks. They have serious impacts over the society in the form of economical disrupt, psychological disorder, threat to National defense etc. Cybercrime plays directly upon the greed and gullibility of people both naïve and otherwise worldly. India may succeed in combating the problem of cybercrimes by adopting a synergetic approach wherein technological measures and proper legislative framework with a properly trained human resource in a tech-savvy society.

Keywords: cyber, internet, Phishing, hacking, cyberspace

1. Introduction

Everybody should want to make sure that we have the cyber tools necessary to investigate cyber crimes and to be prepared to defend against them and to bring people to justice who commit it. Janet Reno[2]

In 1960s internet was developed for better communication and research. With advancement of technology of internet everything becomes easy to access but also provides pathway to commit crimes easily without any effort. Although there exist firewalls, antivirus software, and other technological solutions for safeguarding the data and networks, some human minds of criminal nature use internet as a tool of crime which is now known as cyber crime committed in cyber space. [3]Cyber crime is now the burning issue for all countries to handle because most of data is transferred online even governmental data also. Even most of the seasoned users of IT tools may not be aware of cyber victimization.

Along with the advancements in technology it is equally important to be aware of disadvantages as the cybersafety depends on the knowledge of the technology and the care taken while using internet and that of the preventive measures adopted by user and servers systems. It is well said that the problems created cannot be solved with the same level of awareness that created them. Cyber crime mainly consists of unauthorized access to Data and data alteration, data destruction, theft of funds or intellectual property. Due to these online criminal activities cyberspace is most unsafe place to do business. Word cyber space was first used by William Gibson, in his book, Necromancer, written in 1984. Cyberspace can be defined as a virtual world of computers where internet is involved, where individuals can interact, conduct business, do transactions, develop graphics. Hence there is need to enhance awareness about thecybercrime. Bhushan[4]has revealed that awareness of cybernetics in India is abysmally low and thus has gained a reputation as a country where foreign investors can do business in cybersecurity and have been investing heavily in cybersecurity, stressing need for a centralized management to control Internet, telecom and power sectors. Pandey[5]concluded that lack of awareness about internet and low level of internet security is fast making Indore aheaven for cybercriminals.

According to Dalal[6]one area that requires special attention is the 'cyberlaw awareness' in India.Nappinai[7] found that cybercrime prosecution is not resorted in many instances due to lack of awareness amongst both the victimsand the enforcement authorities about the applicability of general laws to cybercrimes.

* Author for correspondence

Saxena etal[8]have concluded that proactive actions on the part of Government and enhanced participation of education system in the cybersecurity awareness approach may lead to a strongly secured nation. Jamil and Khan[9]while comparing the data protection act in India with that of European countries have concluded that the Indian cyber laws are very poor and it is very necessary to actually bring in the appropriate cyber law and awareness about them.

Seth[10] has noticed that with increasing awareness and provision of training on the subject of cybercrime, enhanced technological and legislative steps being taken to further strengthen the IT laws and enforcement framework, India will effectively succeed in combating the problem of cybercrimes.

2. Current Trends of Cyber Crime

While the vast majority of hackers may be disinclined towards violence, it would only take a few to turn cyber terrorism into reality- Dorothy Denning[11]

Locard's principle of exchange, that anyone or anything entering a crime scene takes something of the scene away and leaves something of themselves behind does not apply generally to the cyber world.

It might apply in some circumstances, but especially is it the case that most computer security systems currently used does not track, trace and generate legally admissible evidence through the systems designed into computers.

2.1 Stalking

Cyber stalking, is one of the most common, is use of the Internet or other electronic means to stalk someone. This term is used interchangeably with online harassment and online abuse. [12]

First stalking case registered in India:

The Delhi Police registered India's First Case of Cyber stalking. One Mrs. RituKohli complained to the police against a person who was using her identity to chat over the Internet at the website www.mirc.com, mostly in the Delhi channel for four consecutive days.Mrs. Kohlifurther complained that the person was chatting on the Net, using her name and giving her address and was talking obscene language. The same person was also deliberately giving her telephone number to other chatters encouraging them to call RituKohli at odd hours.

Consequently, MrsKohli received almost 40 calls in three days mostly at odd hours from as far away as Kuwait, Cochin, Bombay and Ahmadabad. The said calls created havoc in the personal life and mental peace of RituKohli who decided to report the matter.[13]

2.2 Hacking

"Hacking" is a crime, which entails cracking systems and gaining unauthorized access to the data stored in them. Case related to hacking reported:

MUMBAI: Cyber criminals hacked into the Mumbai-based current account of the RPG Group of companies and shifted Rs 2.4 crore. The bank has blocked the accounts of the illegal beneficiaries, but the hackers have already managed to withdraw some funds from them, sources said.[14]

2.3 Phishing

Phishing is just one type of the many frauds on the Internet, trying to fool people into parting with their money.

Case related to phishing: HYDERABAD:

An email allegedly from India's central bank, asking to secure their bank account details with the RBI is fake, and an attempt by new-age fraudsters to con people into giving away bank account details and lose hard-earned money, security experts said.

The email says RBI has launched a new security system, asking users to click on a link to open a page with list of banks in place. Once anyone chooses a particular bank, it asks for all net banking details, including card numbers and the secret three digit CVV number, among others.[15]

2.4 Squatting

Cyber squatting is the act of registering a famous domain name and then selling it for a fortune. This is an issue that has not been tackled in IT act 2000. [16]

2.5 Bot Networks

A cyber crime called 'Bot Networks', where spamsters and other perpetrators of cyber crimes remotely take control of computers without the users realizing the fact that their system is being in use by some fake user.

2.6 Cross Site Scripting (XSS) and Vishing[17]

Cross site scripting Cross-site scripting (XSS) is a type of computer security threat in which malicious users insert some harmful code into the WebPages of trusted web sites viewed by other users.

These were some types discussed but there are many more sides of cyber crimes which falls under IT act 2000[18] and IPC like obscene publication, obtaining license of digital signature by providing false information, breach of privacy, offence against public

GJEIS | Print ISSN: 0975-153X | Online ISSN: 0975-1432

servant, forgery, criminal breach of trust and many more. Some noteworthy amendments in the definition sections include:

The replacement of the word "Digital" with the word "Electronic", which makes the IT Act more technology neutral and expands its applicability beyond just the digital medium.

1. Inclusion of cell phones, personal digital assistants and other such devices in the definition of "Communication Devices" broadens the scope of the statute.
2. The modified definition of "Intermediary" includes all service providers in respect of electronic records again broadens the applicability while inclusion of Cyber cafes in the definition of Intermediaries removes the need to interpret the statute.

The extensive definition of "cyber security" as including protection of both data and the equipment from unauthorized access, use, disclosure etc., is another vital inclusion that impacts the new Data Protection provisions included under the ITA, 2008. The relevance of these definitions, where applicable are set out below.

3. Conclusion and Impact

Lunda Wright, a legal researcher specializing in digital forensic law at Rhodes University, has an interesting research finding on a blog posted in October 2005. It states that there has been an increased rate of prosecutions of cyber-criminals. There has been an increased clamping down on cyber-piracy related to the film and music works. There are novel lawsuits and strategies for litigation. [19]Police departments across the nation validate that they have received an increasing number of such crimes reported in recent years. This is in sync with the national trend resulting from increased computer use, online business, and geeky sophisticated criminals.

In the year 2004, cyber-crime generated a higher payback than drug trafficking, and it is set to grow further as the use of technology expands in developing countries.

3.1 Potential Economic Impact

The 2011 Norton Cyber crime disclosed that over 74 million people in the United States were victims of cyber crime in 2010. These criminal acts resulted in $32 billion in direct financial losses. Many people have the attitude that cyber crime is a fact of doing business online![20]

As today's consumer has become increasingly dependent on computers, networks, and the information these are used to store and preserve, the risk of being subjected to cyber-crime is high. Some of the surveys conducted in the past have indicated as many as 80% of the companies surveyed acknowledged financial losses due to computer breaches. The approximate number impacted was $450 million. Almost 10% reported financial fraud. [21]As the economy increases its reliance on the internet; it is exposed to all the threats posed by cyber-criminals. Stocks are traded via internet, bank transactions are performed via internet, purchases are made using credit card via internet. All instances of fraud in such transactions impact the financial state of the affected company and hence the economy. Productivity is also at risk. These types of consumer trust issues could have serious repercussions and bear going into more detail.

3.2 Impact on Consumer Trust

Since cyber-attackers intrude into others' space and try and break the logic of the page, the end customer visiting the concerned page will be frustrated and discouraged to use the said site on a long term basis. The site in question is termed as the fraudulent, while the criminal masterminding the hidden attack is not recognized as the root cause. This makes the customer lose confidence in the said site and in the internet and its strengths.

According to reports sponsored by the Better Business Bureau Online, over 80% of online shoppers cited security as a primary worry when conducting business over the Internet[22]. About 75% of online shoppers terminate an online transaction when asked for the credit card information.

The perception that the Internet is rife with credit card fraud and security hazards is growing. This has been a serious problem for e-commerce.

Complicating the matter, concern over the credibility of an e-business in terms of being unsafe or cluttered makes a shopper reluctant to transact business.

3.3 Areas Ripe for Exploitation: National Security

Cyber attacks are not what make the cool war 'cool'. As a strategic matter, they do not differ fundamentally from older tools of espionage and sabotage -Noah Feldman[23]

Modern military of most of the countries depends heavily on advanced computers. Information Warfare, or IW, including network attack, exploitation, and defense, isn't a new national security challenge, but since 9/11 it has gained some additional importance. IW appeals because it can be low-cost, highly effective and provide deniability to the attacker. It can easily spread malware, causing networks to crash and spread misinformation.[24] The Internet has 90 percent junk and 10 percent good security systems. When intruders find systems that are easy to break

into, they simply hack into the system. Terrorists and criminals use information technology to plan and execute their criminal activities. Cyber war takes place largely in secret, unknown to the general public on both sides. The increase in international interaction and the wide spread usage of IT has facilitated the growth of crime and terrorism.

4. Reference

1. Anna Maria Chavez is the Chief Executive Officer of the Girl Scouts of the USA and the first Latina to head the organization.
2. served as the Attorney General of the United States, from 1993 to 2001
3. Dr. Vijay Kumar Shrikrushna Chowbe, The concept of Cyber Crime:Nature& Scope.
4. Bhushan K. India ranks fifth among cybercrime affected country. 2012. Available at: http://www.thinkdigit.com/Internet/India-ranks-fifth-among-cyber-crimeaffected_9476.html
5. Pandey K. Low security makes natives vulnerable to cyber crimes. 2012. Available at: http://articles.timesofindia.indiatimes.com/indore/31863717_1_cyber-crimes-cyber-cellcyber-criminals
6. Dalal P. Awareness of Cyber Law in India. 2010. Available at: http://cyberlawsinindia.blogspot.in/2010/05/awareness-of-cyber-law-in-india.html
7. Nappinai NS. Cyber Crime Law in India: Has Law Kept Pace with Emerging Trends? An Empirical Study. N. S. Journal of International Commercial Law and Technology. 2010; 5(1).
8. A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India. IACSIT International Journal of Information and Education Technology. 2012; 2(2).
9. Data Protection Act in India with Compared To the European Union Countries. International Journal of Electrical & Computer Sciences. 2011; 11(6).
10. Seth K. India – Cyber crimes and the arm of Law – An Indian Perspective. 2007. Available at: http://www.sethassociates.com/%E2%80%9Ccyber-crimes-and-the-arm-of-law-anindian-perspective.html
11. Dorothy Elizabeth Denning is an American information security researcher.
12. Ebel RL. Educational tests and measurements; Examinations; Evaluations; Design and Construction. Interpretation (3e), Prentice Hall, New Jersey: Englewood Cliffs; 1979.
13. Report by Pawan Duggal, Cyber law consultant, president, cyber-laws.net
14. Times of India, Mumbai bank hacked, Rs 2.4 crore siphoned off in 3 hours. May 18, 2013.
15. Times of India, Now, a phishing email in the name of RBI. May14, 2013.
16. Vishing The name comes from "voice," and "phishing," Vishing is the act of using the telephone in an attempt to scam the user. Which is, of course, the use of spoofed emails designed to trap targets into clicking malicious links that leads to a toll free number?Instead of email, vishing generally relies on automated phone calls, which instruct targets to provide account numbers for the purpose of financial reward. How vishing scams work:Criminals set up an automated dialing system to text or call people in a particular region or area code (or sometimes they use stolen customer phone numbers from banks or credit unions). The victims receive messages like: "There's a problem with your account," or "Your ATM card needs to be reactivated," and are directed to a phone number or website asking for personal information. Sometimes criminal quote some information about your account before asking you to enter information, so you could believe its an authenticated source.
17. The Hindu, "a new squatting case registered under ACPA", February 13th, 2013.
18. Nappinai NS. Cyber Crime Law in India: Has Law Kept Pace With Emerging Trends. Journal of International commercial Law And Technology. 2010; 5(1).
19. Nigel Jones, Director or the Cyber Security Knowledge Transfer Network, was featured in the daily telegraph (May 6, 2008), Cyber Security KTN.
20. Coleman KG. Cyber Intelligence: The Huge Economic Impact of Cyber Crime. 2011. Available at: http://gov.aol.com/2011/09/19/cyber-intelligence-the-huge-economic-impact-of-cyber-crime/, Visited: 28/01/2012
21. PTI Contents, India: A major hub for cybercrime. 2009. Available at: http://business.rediff.com/ slide-show/2009/aug/20/slide-show-1-india-major-hub-for-cybercrime.html
22. Report on Cyber Crime-chapter 18- NCRB reportwww.ncrb.gov
23. Noah Feldman is an American author and professor of law at Harvard Law School.
24. Yassir A, Nayak S. Cyber Crime: Threat to Network Security. IJCSNS. 2012 Feb; 12(2).