Effect of Cyber Crime Indian Economy

Yerra Shankar Rao[1] Dr Hemarj Saini[2] Dr T.C.Panda[3]
[1]Ph.D.Schlor [2]Assistant Professor [3] Principal
[2]Department of Computer science and Engineering & Information and Communication Technology
[1]SOA University BBSR [2]jaypee University of Information Technology (Juit), Waknaghat, Solan, Himachal Pradesh, India [3]OEC BBSR

Abstract— *A lot of people in the world, mostly Indian have a limited knowledge of the crime occurring in cyberspace, known as cybercrime. Cybercrime happens in the world of computer and the Internet. This kind of crime has a severe impact on our economy, lives and society, because our society is becoming an information society, full of information exchange that is happening in cyberspace. Our research work is aimed at knowing the level of awareness of individuals on the existing phenomenon in India, and their impacts on India economy. A survey was carried out with the aims of getting these results using questionnaire as an instrument, the responses were quantitatively analysed using some statistical techniques. The results show that cracking, software piracy, and pornography among others are prevalent crimes in India. While the impacts of these crimes on Indian economy cannot be over emphasized. Recommendations were proposed on how these crimes can be minimized if not totally eradicated. Cyber crime, especially in India is growing at the rate of 50% per year and the number of incidents of cyber crimes is increasing day by day. India ranks fifth in the incidents of cyber crimes in the world.*

Keywords— e-crime, cyber crime, internet, computer hacking, pornography, identity loss, hacking, economics impact

I. INTRODUCTION

A crime is an offense that may be prosecuted by the state and punishable by law. A cyber crime is a type of crime which uses computers and networks as target or weapon. Today's necessity is to minimize the cyber crimes occurring in various parts of the world. Cyber crimes in India are increasing at an alarming rate. It will be better if the rate of occurrence of cyber crime patterns is predicted for various parts of the countryCyber crime began with disgruntled employees causing physical damage to the computers they worked with, with the aim to get back at their superiors. As the ability to have personal computers at home became more accessible and popular, cyber criminals began to focus their efforts on home users[1]. Further research on this reveals that history of cybercrime was further established that the first published report of cybercrime occurred in the 1960s, when computers were large mainframe systems. Since mainframes were not connected with other ones and only few people can access them, the cybercrimes were always "insider" cybercrimes, which means employment, allowed them to access into mainframe computers, and then refers to as computer crime rather than cybercrime. Actually, in the 1960s and 1970s, the cybercrime, which was "computer crime" in fact, was different from the cybercrime we faced with today, because availability of Internet was restricted within some sections (e.g. US military) in that era. In the following decades, the increasing of computer network and personal computers transformed "computer crime" into real cybercrime. In fact, the former descriptions were "computer crime", "computer-related crime" or "crime by computer". With the pervasion of digital technology, some new terms like "high-technology" or "information-age" crime were added to the definition. Since Internet was invented, other new terms, like "cybercrime" and "net" crime became the order of the day as people began to exchange information based on networks of computers, also keep data in computer rather than paper. At the same time, the cybercrime was not only restricted in target cybercrime, but expanded into tool cybercrime and computer incidental. We therefore come to terms with a conclusion on the meaning that cybercrime is an evil having its origin in the growing dependence on computers in modern life. A simple yet sturdy definition of cybercrime would be unlawful acts wherein the computer is either a tool or a target or both". Defining cybercrimes as illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them. Cybercrime in a broader sense computer-related crime: any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.[5]

Cyber Crime refers to all activities done with criminal intent in cyberspace. These fall into three categories:

Cyber crime against the persons Cyber Crimes against Business and Non-business organizations' Crimes against the government.

cyber crime has transformed into a money spinner business that yields hundreds of millions of dollars and involves lesser risk than traditional crimes. Cyber crime, especially in India is growing at the rate of 50% per year and the number of incidents of cyber crimes is increasing day by day. India ranks fifth in the incidents of cyber crimes in the world

Meanwhile, in an attempt to uncover these crimes billions of India is lost through these crimes annually with little or no hope of curbing it due to its complex nature. Most perpetrators of this crime are never caught and if at all caught, are never prosecuted because of lack of concrete evidence, organizational and societal awareness. As a result the extent and impact of Cybercrime is uncertain because lack of reporting leads to uncertainty with regard to the extent and impact of the crime. This is especially relevant with regard to the involvement of these crimes as compared to other organized crimes. Available information from the crime statistics in India is lacking and if any, do not reflect

the real extent or impact of this crime in our every-day living.

II. LITERATURE REVIEW

A. What is Cybercrime?

In the most general form crime can be de-fined as the violation of law, especially a serious one Cyber crime is an unlawful act wherein the computer is either a tool or target or both. Cyber crime consists of specific crime dealing with computer and networks and facilitation of traditional crime through the use of a computer. Cyber crime uses the unique feature of Internet namely the sending of emails, speedy publication of information through the web to any one the planet. These criminal activities can often be faster [7]

A cybercrime is a crime that is committed with the help of a computer through a communication device or a transmission media called the cyberspace and global network called the Internet [2]. Cyber crime has been increasing in complexity and financial costs since corporations, government and individual or society at large started utilizing computers in the course of doing business. As technology increases between governments, corporate organizations and individuals that are involved in international and local businesses; criminals have realized that this is a cost effective method to make money. Efforts to address Internet crime include activities associated with defending networks and data, detecting criminal activities, inquiring into crime and taking legal action against criminals [3].Cyberspace security is crucial for maintaining the continuity of these vital services and for preserving the public‟s trust in information systems. But can this be achieved world-wide? Well, this is a topic for another day as our focal point in this paper is all about cybercrimes and its impact on the Indian economy.[6]

Some examples of cyber crimes include sending spam emails (spamming), stealing personal information (identity theft), breaking into someone's computer to view or alter data (hacking) and tricking someone into revealing their personal information (phishing), making Internet services unavailable for users (Denial of service –DOS), advanced free fraud 419 (aka Yahoo-yahoo), credit card fraud (ATM), plagiarism and software piracy, pornography, stealing money bit-by-bit in a cunning way (salami attacks) and virus dissemination etc.So many crimes are committed every day in the Indian cyberspace. A recent report in the Daily Trust, (2010)by the Internet Crime Complaint Centre, which is a partnership between the Federal Bureau of Investigation (FBI) and America's National White Collar Crime Centre, revealed that India is now ranked third among the list of top ten sources of cybercrime in the world with 8% behind the US (65%) and the UK (9.9%). [5]. What Indian government, corporate organizations and the society at large do not know is that the heavy economic impact on the country, (either in financial terms or otherwise), will have an adverse consequences on unemployment rate, social services and international reputation.

Therefore, a detailed introduction of cybercrime needs to be presented with the view to fully analyze the indices that make up this crime so that our government and society will be aware of this crime and its implication on the economy. In this paper, we will introduce the origins and the evolution of cybercrime, the different categories of cybercrime (target cybercrime, tool cybercrime and computer incidental).

The impact of cybercrime has been, and will be in the future, felt by all governments and economies that are connected to the Internet. Criminals will use the Internet, computers and other digital devices to facilitate their illegal activities as long as the financial gains outweigh the consequences when caught. Knowing about the quantity of Cybercrime as well as the economic impact is vital for both governments as well as businesses which could be a necessary tool to adjust the legal and regulatory frameworks as well as institutional capacities. Prosecutors and law enforcement agencies must have resources, training and equipment required to address cybercrime in order to keep current on this newest method of crime fighting. Lack of reporting this crime leads to uncertainty with regard to the extent and impact. This is especially relevant with regard to the involvement of organized crime. Available information from the crime statistics in India, if at all available, does not reflect the real extent of the crime or damages cause as a result of the crime. Different motivations of private users and businesses not to report Cybercrime is another concern for the Government [9].

What is known is that the losses caused by Cybercrime can be significant. Losses are not only related to direct financial losses but also necessary investments in Cyber security and loss of reputation when incidents happen. It is important to give guidance in this regard e.g. reporting obligation / establishment of reporting mechanisms (complaint center) [8].

B. Types of Cybercrimes most prevalence in Indian

(1) Assault by Threat – threatening a person with fear for their lives or the lives of their families or persons whose safety they are responsible for (such as employees or communities) through the use of a computer network such as email, videos, or phones.
(2) Child pornography – the use of computer networks to create, distribute, or access materials that sexually exploit underage children.
(3) Cyber laundering – electronic transfer of illegally-obtained monies with the goal of hiding its source and possibly its destination.
(4) Cyber stalking – express or implied physical threats that creates fear through the use of computer technology such as email, phones, text messages, webcams, websites or videos.[3]
(5) Cyber terrorism – premeditated, usually politically-motivated violence committed against civilians through the use of, or with the help of, computer technology. [9]
(6) Cyber theft is using a computer to steal. This includes activities related to: breaking and entering, DNS cache poisoning, embezzlement and unlawful appropriation, espionage, identity theft, fraud, malicious hacking, plagiarism, and piracy.

– Hardware Hijacking - Researchers at Columbia University recently discovered a serious security flaw in certain printers, as well. Many printers automatically update their software when accepting

a print job, connecting to the Internet to download the latest print drivers.

- Spam - Unsolicited mass e-mail, known colloquially as "spam", is more than annoying: spam messages can be used to trick people into giving up sensitive personal information (known as "phishing"), or as carriers for computer worms and viruses. [1]
- Script kiddies-A wannabe hacker. Someone who wants to be a hacker (or thinks they are) but lacks any serious technical expertise. They are usually only able to attack very weakly secured systems.
- Insiders- They may only be 20% of the threat, but they produce 80% of the damage. These attackers are considered to be the highest risk. To make matters worse, as the name suggests, they often reside within an organization

(7) Yahoo Attack:- Also called 419 because section 419 of the Indian criminal code has a law against such offenders. It is characterized by using e-mail addresses obtained from the Internet access points using e-mail address harvesting applications(web spiders or e-mail extractor). These tools can automatically retrieve-mail addresses from web pages. Indian fraud letters join the warning of impersonation scam with a variation of an advance fee technique in which an e-mail from Indian offers the recipient the chance to share a percentage of a huge amount of money that the author, a self-proclaimed government official, is trying to siphon out of the country

(8) Salami Attack:-Salami assaults are flamboyant economic scams or exploits against confidentiality by comprehensive data gathering.[9]

III. Methodology Of The Research

The method we employed in this research was the survey method while the research design used was the purposive research design technique so as to meet up with the targeted presentation date. The survey method was used because our aims are to get the awareness from users of the computer vis-a-viz the Internet and to determine the impacts of these menaces on the economy The population of this study is the Mathematics Department and Computer Science Department of Centurian University in order to get the impacts from the professional while the Computer and Internet users mostly students and Lecturers. A sample size of 60 was selected using the random sampling procedure from the targeted population of 120. The method used to collect data for this study is structured questionnaire. A total of 60 copies of the questionnaire were personally administered out of which 55 copies were retrieved in usable form. This represents a response rate of 91.6%. [6]

IV. Analysis Of Data

The responses to the questions in the questionnaire provided the basis for the following analysis. The key to the table are SA: strongly agree, A:agree, U: undecided, D: decided, and SD: strongly decided

Types of Cyber crimes	Options	Frequency	Percent
Cracking	SA	29	52.7
	A	24	43.6
	U	1	1.8
	D		
	SD	1	1.8
	Total	55	100
Software Piracy	SA	29	52.7
	A	17	30.9
	U	2	3.6
	D	5	9.1
	SD	1	1.8
	Missing	1	1.6
	Total	55	100
Pornography	SA	22	40
	A	18	32.7
	U	4	7.3
	D	4	7.3
	SD	5	9.1
	Missing	2	3.6
	Total	55	100
ATM fraud	SA	29	52.7
	A	17	30.9
	U	2	3.6
	D	2	3.6
	SD	4	7.3
	Missing	1	1.8
	Total	55	100
Yahoo yahoo/extortion	SA	25	45.5
	A	21	38.2
	U	1	1.8
	D	2	3.6
	SD	5	9.1
	Missing	1	1.8
	Total	55	100

Table 1: Perceived awareness level of respondents to cyber crimes Source: Field survey

From the table 1. It shows clearly that cracking is a major crime in our society with the frequency of 29 and percentage of 52.7% while the least which was strongly disagree went for 1 with a percentage 1.8%. This improvement may not be too far from the fact that Internet is almost available for every user. Almost the same level of awareness goes for pornography, software piracy and ATM fraud with the frequencies of 22, 29 and 29; and percentages of 40%, 52.7%, 52.7%. It won't be out of place if we assume that the increment in all these mentioned cases are also as a result of the availability of Internet connectivity. Another prominent cyber crime we have in our society today is the yahoo-yahoo (cyber extortion) which seem uncontrollable, table 1 shows that 25 respondents strongly agreed that it is a noticeable crime with a percentage of 45.5% while only 1 respondent remained undecided with a percentage of 1.8%. Despite the high level of benefits derived from the use of the Internet, it almost seems the disadvantages are appearing to be overwhelming.

V. Conclusion

In India, there is no doubt that a good number of people have turned the ethical use of information and communication technologies into unethical activities. This problem is not peculiar to India alone, but it is a problem world-wide and that is why it becomes imperative that organizational data /information must be safeguarded especially these days that almost every business is being run

on line. our investigation on cybercrimes we observed its threat to the economy of a nation and even peace and security. Therefore there is need for a holistic approach to combat these crimes in all ramifications. Our proposal therefore is the need for cyber police who are to be trained specially to handle cybercrimes in India. In addition, the police should have a Central Computer Crime Response Wing to act as an agency to advise the state and other investigative agencies to guide and coordinate computer crime investigation. We are also proposing that the country should set up National Computer Crime Resource Centre, a body, which will comprise experts and professionals to establish rules, regulations and standards of authentication of each citizen's records and the staff of establishments and recognized organization, firms, industries etc.Forensics commission should be established, which will be responsible for the training of forensics personnel/law enforcement agencies. Above all, comprehensive law to combat computer and cyber related crimes should be promulgated to fight this phenomenon "to a halt. Our proposal on the nature of law to combat cybercrime is not included in this paper. We recommend that before anybody enters into any kind of financial deals with anyone through the internet he/she should use any of the search engines to verify the identity of the unknown.

REFERENCES

[1] Shinder, D.L.(2002), Scene of the Cyber crime: Computer Forensics Handbook. Syngress Publishing Inc. 88 Hingham Street, USA
[2] Types of cyber crime, http://www.slideshare.net/ferumxxl/types-of-computer-crimes. Accessed on December 2012
[3] Criminal Investigation Department Review, January 2 (Mis Cyber Crime Scenario In India Criminal Investigation Department Review January 19 , 2008
[4] Hawser, A. (2011). Hidden threat. Global Finance, 25(2), 44
[5] Milner, H. V. (1999). The political economy of international trade. Annual Review of Political Science, 2, 91–114
[6] Conference proceedingby Yerra Shankar Rao "Cyber crime Assement "National Conference on Current Trends in Computing (NCCTC) ISBN No. : 978-3-642-24819-6, 23rd -24th March, 2014 ,Page no10-14.,North Orissa University ,Baripada Orissa
[7] India emerging as major cyber crime centre (2009), Available at: http://wegathernews.com/ 203/india-emerging-as-major-cyber-crime-centre/, Visited: 10/31/09
[8] By Jessica Stanicon (2009), Available at: http://www.dynamicbusiness.com/articles/articles-news/one-in-five-victims-of-cybercrime3907.html, Visited: 28/01/2012
[9] Hemraj saini,Yerra Shankar Rao,T.C.Panda " Cyber crime and their Imapct A Review" IJERA March 2012 ,Vol 2 P.P No 201-206