Kijsanayoth. Cyber-security analysis of smart SCADA systems with game models. Proceedings of the 9th annual cyber and information security research conference, ACM, 2014, pp. 109–112.

7. Von Solms, Rossouw, Johan Van Niekerk. From information security to cyber security. Computers and Security. 2013; 38: 97–102.

8. Eric A. Fischer. (2106). Cybersecurity Issues and Challenges: In Brief. [Online]. Available from https://fas.org/sgp/crs/misc/R43831.pdf [Accessed on October 201

❑❑❑

34

An Impact of Cyber Crime Indian Economy

Dr.Rodage Kailas Dadasaheb
Assistant Professor in Economics,
Dada Patil College Karjat, Tal-Karjat,
Dist.A.Nagar

****

Abstract:

Cybercrime is relentless, undiminished, and unlikely to stop. It is just too easy and toCybercriminals at the high end are as technologically sophisticated as the most advanced information technology (IT) companies, and, like them, have moved quickly to adopt cloud computing, artificial intelligence, Software-as-a-Service, and encryption. Cybercrime remainsfar too easy, since many technology users fail to take the most basic protective measures,and many technology products lack adequate efenses, while cybercriminals use bothsimple and advanced technology to identify targets, automate software creation anddelivery, and monetization of what they steal.

The aim of the research is to examine the negative impact cybercrimespose to the society. The concepts of cybercrimes are introduced and different typesof cybercrimes are explored as examples of some of the impacts which caused bycybercrimes activities. Results from this study show that, there are many negativeimpacts which the society suffer from the cybercrimes and why the computer ornetworking are tools target for the crimes. The discussions are made from thefindings and finally the paper addresses different measures which can be taken tocombat these cybercrimes so that people still enjoy using the technology rather thanstop them to use it.

1. Introduction

As the Internet came into widespread commercial use, the nature of computercrimes began to shift. 'While in some crimes, one component of the crime may havebeen committed using an electronic instrument, in other crimes, the crime as awhole is committed in the online or electronic environment. These crimes, knownas cybercrimes, generally occur in the virtual community of the Internet or incyberspace' (Heather 2008, Newton 2008).

Viruses, worms, and Trojan horses are another serious threat. There is a variety ofCyber crime committed but these are the most prevalent and appear to be among themost troubling to computer users (Furnell, 2002 in Brett, 2008).

As it has been seen in the introductory part, there is no way any organization orcountry can avoid the uses of ICT since it needs to remain competitive in the marketplace, but the biggest issue is how to deal with cybercrimes so as to minimizeif not to reduce its threats. Therefore, the paper intends to explore the impact ofcybercrimes in the society and the security measures which can be taken to prevent these threats.

The wide range of existing estimates of the annual loss—from a few billion dollars to hundreds ofbillions—reflects several difficulties. Companies conceal their losses and some are not aware of what hasbeen taken. Intellectual property is hard to value. Some estimates relied on surveys, which provide veryimprecise results unless carefully constructed. One common problem with cybersecurity surveys is thatthose who answer the questions "self-select," introducing a possible source of distortion into the results.

Given the data collection problems, loss estimates are based on assumptions about scale and effect—change the assumption and you get very different results. These problems leave many estimates opento question.

The Components of Malicious Cyber Activity

In this initial report we start by asking what we should count in estimating losses from cybercrime and cyber espionage. We can break malicious cyber activity into six parts:

- Opportunity costs, including service and employment disruptions, and reduced trust for online activities
- The loss of sensitive business information, including possible stock market manipulation
- The additional cost of securing networks, insurance, and recovery from cyber attacks
- Cybercrime, which costs the world hundreds of millions of dollars every year
- The loss of intellectual property and business confidential information
- Reputational damage to the hacked company

2. Objective of the Study

1. To evaluate the Problems will rise up within the Cybercrime in society.
2. To assess the which may include authenticity and non-repudiation
3. To evaluate Cybercrime has been increasing in complexity and financial costs

3.Research Methodology

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 Commerce , Economics, Computer Science Department of (SPPU)University of Pune in order to get the impacts from the professional while the Computer and Internet users mostly students and Lecturers. A sample size of 50 was selected using the random sampling procedure from the targeted popula-

tion of 100. The method used to collect data for this study is structured questionnaire. A total of 50 copies of the questionnaire were personally administered out of which 46 copies were retrieved in usable form. This represents a response rate of 92%. [6]

4. 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 publics 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].

5. 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.

a. 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.

b. 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]

c. 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.

d. 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]

6.Analysis of Data

The responses to the questions in the questionnaire provided the basis for the following analysis. *Perceived awareness level of respondents to cybercrimes Source:

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 cybercrime we have in our society today is the yahoo-yahoo (cyber extortion) which seem uncontrollable,

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.

7. 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

· Shinder, D.L.(2002), Scene of the Cyber crime: Computer Forensics Handbook.

Syngress Publishing Inc. 88 Hingham Street, USA

· Eric A. Fischer. (2106). Cybersecurity Issues and Challenges: In Brief. [Online]. Available from https://fas.org/sgp/crs/misc/R43831.pdf [Accessed on October 201

· 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

· Manmohan Chaturvedi, AynurUnal, ShilpaBahl. International cooperation in cyber space to combat cyber crime and terrorism. 2014 IEEE Conference on Norbert Wiener in the 21st Century (21CW). IEEE, 2014.

· Milner, H. V. (1999). The political economy of international trade. Annual Review of Political Sci-ence, 2, 91–114

· Martin, Nigel, John Rice. Cybercrime: Understanding and addressing the concerns of stakeholders. Computers and Security. 2011; 30(8): 803–814.

· Conference proceedingbyYerra Shankar Rao "Cyber crimeAssement "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

· Sergey, Melnik, Smirnov Nikolay, Erokhin Sergey. Cyber security concept for Internet of Everything (IoE). Systems of Signal Synchronization, Generating and Processing in Telecommunications. 2017. IEEE, 2017.

· Shang H, Jiang R, Li A. A Framework to Construct Knowledge Base for Cyber Security. 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC). IEEE, 2017.

· India emerging as major cyber crimecentre (2009), Available at: http://wegathernews.com/ 203/india-emerging-as-major-cyber-crime-centre/, Visited: 10/31/09

· Rayne Reid, Johan Van Niekerk. From information security to cyber security cultures. Information Security for South Africa (ISSA). 2014. IEEE, 2014.

· R. Hewett, S. Rudrapattana, P. Kijsanayoth. Cyber-security analysis of smart SCADA systems with game models. Proceedings of the 9th annual cyber and information security research conference, ACM, 2014, pp. 109–112.

· Types ofcyber crime, http://www.slideshare.net/ferumxxl/types-of-computer-crimes. Accessed on December 2012

· Von Solms, Rossouw, Johan Van Niekerk. From information security to cyber security. Computers and Security. 2013; 38: 97–102.

❑❑❑