A Review on Recent Computer Crimes

Nidhi Sethi
Renaissance Institute of Professional Studies, Indore, M.P., India
nidhisogani@gmail.com

Abstract: **With the evolution of technology, crimes happening with the help of computer and internet are increasing day by day and have become curse for the modern era. Cybercrime globally affects IT environment very much be it government, companies, banking or individuals. This paper gives the rigorous review and revision of the various categories of cybercrime along with their social-economic impact.**

Key words: Cybercrime, Cyber terrorism, Cyber bullying

I. INTRODUCTION:

Before a past few decades the crimes on internet was unheard. Due to diverse online activities of common man of shopping, banking, education, entertainment, e- governance to name a few has introduced the term computer crimes. Also with rapid expansion of businesson internet leads to the various computer crimes. Computer crimes also termed as cybercrime are the illegal activities performed with malicious intentions by group of users with the help of computers and internet.The problem of computer crimes is not limited to just hacking government, business, individual sites now it has been enlarged with social media, smart phones so needs to be addressed precisely. Now a day almost the whole world is victim of these crimes and the costs pertaining to handle cybercrimes are also increasing rapidly. Thus it has become a global issue to be researched. .

Although a lot of research work has been carried out on computer crimes but still it is lacking the systematic review and organization. Researchers have different views pertaining to e crimes. Thus this paper focuses on detailed classification of the e crimes and its impact with social and economic perspective.

This paper is divided in to four section first section gives the related work that has carried out, the next section talk about various categories of these e crimes. Further this paper discusses about their impact on various streams. Last section concludes the paper with the future work and scope.

II. RELATED WORK:

Cybercrimes is not a new term. Lot many research has been carried out by different researchers some of them are listed here. Initially Anthony Riem proposed the "Cybercrimes Of The 21st Century" in this he has described various cybercrimes that are being practiced against businesses.

In 2010 Alex Roney Mathew, Aayad Al Hajj, Mohammed Ambusaidi proposed the "Cybersquatting" definition and law controlling the cybersquatting.In 2013 Sumanjit Das and Tapaswini Nayak proposed a paper "Impactof Cyber Crime: Issues and Challenges" in this paper they have given so many fact and figures of the various crimes and also discussed about the future challenges of cybercrimes. Folashade B. Okeshola, Abimbola K. Adeta in 2013 proposed "The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions In Zaria-Kaduna State, Nigeria" they have analyzed cybercrimes in only a specific region.

III. CATEGORIES OF CYBERCRIMES

A. Cyber Terrorism

Cyber terrorism is a kind of attack with a computer and internet as a weapon and an IT expert. It is intended to harm infrastructures of society, such as telecommunications, water supply, and economic and financial institutions to name a few.

B. Stock Market Manipulation:

It is an attempt to create false and artificial market place by inflating or deflating the price of securities/commodities to gain the market power. It can be intended for breaking down or for high close of market to gain the dominance of market. It can be achieved with churning, bear raid, wash trade, ramping and pump and dump.

C. Child predation:

Child predation is described as an act of sexual abuse with a child through internet. It is a very serious threat to young ones. As today's child spent so much time with internet and utilizes numerous online services.It can happen in chat rooms, instant messaging, and e mails and also in social connecting website. A predator is intended to obtain the sexual/personal information in order to either blackmail the child or has wrong intentions of some kind of exploitation.A predator can also insist the child to see the pornographic website and can insist for sexual relationships.

D. Domain squatting:

Domain squatting is termed as the misuse of domain names with bad intentions to resell it at very high prices. Domain name is the actually the unique address of a registrant to a business or company. Domain squatting has been drastically increased with the use of social networking website. It not only misuses the domain name but can also occupy company's trademarks.

E. Denial of service attack:

It is an explicit attempt made by cyber criminals to overload a system with so many requests to loss the network connectivity and to halt other services. Due to this attack system cannot handle the normal requests which are usually handled. So many types of attacks come under the category e.g. Buffer overflow attack, Smurf Attack, Teardrop Attack, SYN Attack etc.

F. Botnet Attack:

It is also known as distributed denial of service attack. In this criminal first takes control of each machine termed as bot (infected machine). Then these bots are organized into a network (botnet) and use these networks to send spams and malwares. The important point is this whole activity happens without the user's knowledge.

G. Cyber bullying

Cyber bullying is a form of bullying which occurs online; through social networking sites, gaming or chat rooms or through mobile phone and tablets. Cyber bullying takes many forms. It can include: Harassment, Denigration, Flaming, and Exclusionand to pressurize someone to send sexual images or pictures.

H. Spam and phishing

These are earlier techniques used in computer crimes. Phishing means illegally obtain sensitive information by deceiving the users. Spam is sending the junk mails to large number of users in order to cheat or steal some credentials from them.

I. Virtual Theft

It is a practice of stealing confidential information (personal, sensitive) through web. It includes identity theft, intellectual property theft, and unauthorized access, telecommunication theft. It is generally done by rivals or competitors with intentions to gain financial benefits from the owner.

J. Cyber extortion

It is a kind of crime done by the group of users to take ransom money against the confidential information of a person or enterprise. In cyber extortion money can be asked for stopping a cyber-attack which was earlier done at large scale. Cyber extortion can be at country level asking government to perform any particular task.

K. Computer based Drug trafficking

It is a kind of illegal business of drugs (having illegal substance) involving worldwide distribution and sale of it. This activity is also taking advantage of internet for making deals. Internet is also used in tracking the products delivery status. Drug trade with virtual exchanges has reduced the face to face communication and thus drug traffickers can easily and comfortably make purchases, distribution and sales also.

IV. SOCIOAL- ECONOMIC IMPACT

Impact of computer crimes has wide dimension. These days not a single field remained unaffected by the computer crimes. These e crimes affect a major part of population of world i.e. youth. It has a varied impact on personal, social and economic perspectives of youth. If we think of personal impact of cybercrimes like cyber bullying, child predation, online pornography, it can break down the relationships of concerning youths. It affects psychologically, decreases Morales, increases frustrations, it also reduces the productivity.It can also destroy the social reputation and can leads to the suicide. Although in business internet has brought the tremendous growth. But above mentioned e crimes like intellectual property right, trademarks infringement, domain squatting to name a few decreases the financial growth of business and also spoils the business reputation. Cyber terrorism and cyber extortion are the today's serious threats to the whole internet community. As everything one can think,be it a business, government projects, banking are handled with the help of internet. So keeping them secured from malicious people is a big challenge. Computer attacks like botnet attack DOD attack, stock market manipulation, virtual theft of telecommunication data and many more cybercrimes can destroy the whole infrastructure of the country if not handled carefully. They can also stop the economic growth of the country. Thus at last we can say all the computer crimes are a big threat to the whole community which is directly or indirectly linked with computer and internet.

V. CONCLUSION

As the cases of computer crimes are increasing day by day. The concern for it should be at first priority keeping this in mind wehave analyzed of computer crimes and their impact. Hundreds of research has been carried in the field thus it is quite difficult to cover everything in a single paper with a limited knowledge. So in this paper we have examined the breadth of e crimes in different dimension. We have also examined their impact on different social and economic perspectives. The paper will be very helpful to all the researchers and academician who want to do something innovative in the field.

REFERENCES

[1] Sumanjit Das, Tapaswini Nayak,“ IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES” International Journal of Engineering Sciences & Emerging Technologies, October 2013. ISSN: 22316604 Volume 6, Issue 2, pp: 142-153

[2] Mohammad Mostufa Kamal, Iqbal Ahmed Chowdhury, Nadia Haque, Mydul Islam Chowdhury &Mohammad Nazrul Islam,” Nature of Cyber Crime and Its Impacts on Young People: A Case fromBangladesh” Asian Social Science; Vol. 8, No. 15; 2012ISSN 1911-2017 E-ISSN 1911-2025

[3] Wojciech Mazurczyk, Thomas Holt,Krzysztof Szczypiorski, “Guest Editors’ Introduction: Special Issue on Cyber Crime”,IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 13, NO. 2, MARCH/APRIL 2016

[4] Dr. Matthew Williams &Dr. Olivia Pearson,” Hate Crime and Bullying inthe Age of Social Media” Conference Report,Cardiff University

[5] Dr. Mike McGuire (University of Surrey) and SamanthaDowling (Home Office Science), “Cyber crime: A review of the evidence,Chapter 1: Cyber-dependent crimes” Home Office Research Report 75 October 2013

[6] Alex Roney Mathew ; Department of Information Technology, Ministry of Higher Education, Nizwa, Sultanate of Oman, Oman ; Aayad Al Hajj ; Mohammed Ambusaidi,”Cybersquatting”, Educational and Information Technology (ICEIT), 2010 International Conference on (Volume:1), Page(s):V1-10 - V1-13 E-ISBN :978-1-4244-8035-7

[7] Aaron G., Bostik K. (2008) "Protecting the web: Phishing, malware, and other security threats", Proceeding of the 17th International Conference on WWWeb 2008