Review of Cyber-Crimes And Their Impacts Over The Society

Umesh R. Gadhave **Dr. Sandeep R. Sirsat**

Abstract- **Due to the increasing use of Internet a huge number of cyber crimes are occurred and it is very difficult to know their behavior as well as understand them hence it is difficult to restrict the victimization in the early phases of the cyber attacks. Cyber attacks may have some motivation behind it or may be processed unknowingly. The attacks those are processed knowingly can be considered as the cyber crime and they have serious impacts over the society in the form of economical disrupt, psychological disorder, threat to National defense, social nuance etc. Restriction of cyber crimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society**.

I. INTRODUCTION

Internet has proven to be a highly dynamic means of communication, reaching an ever-growing people worldwide. The Internet system includes and connects local, regional, national and international networks. The benefits of Internet or Network technology are numerous, starting with its unique suitability for sharing information and ideas. The expansion of the Computer Network made likely the accomplishment of large improvement in research, surgery, expertise, and communication. The modern advance communication technologies have made it possible to communicate with any person in the world in different ways like text massages, chatting on websites by using the access to internet. Mostly for the communication purpose the social networking websites are used. The popularity of social media has grown rapidly in recent years. The famous social networks are Facebook, What's App and other popular networks such as Twitter, Instagram, Orcut, LinkedIn, etc. Now a day's Social-media technologies are used for different purpose including magazines, Internet forums, weblogs, social blogs, social networks, podcasts, photographs or pictures, video, rating and social bookmarking.

Unfortunately the benefits of social networking sites or application also create some problems that affect the security of internet users. Now a day, we are vulnerable to many threats, including: cyber-bullying, spam, fraud, and sexual harassment among others. This technology has allowed some teens to take the bullying that thrives in school hallways into cyberspace.

Users increasingly rely on the trustworthiness of the information exposed on Online Social Networks. Social Network providers base their business models on the marketability of this information. However, Social Networking sites are suffering from abuse in the form of the creation of fake accounts, nuance creating massages, picture which does not correspond to real humans. This can introduce spam, manipulate online rating, or exploit knowledge extracted from the network. This type of things are happened due to popularity of online social networking services such as Facebook, Twitter, Digg, LinkedIn, Google+ etc.

II. RELATED WORK

A number of techniques have been evolved for prevention of the crime over the internet. One of them is a social-graph-based mechanism that enables to a user to identify fake accounts; another technique is CAPTCHA useful for identification of suspicious accounts.

However, none of them proves to be sufficient to fully address this ever-increasing and ever-changing problem.

Vineet Kandpal and R. K.[1] Singh suggested some techniques to minimize the security risk of Cyber crime. They explain the security measures for preventing measures of the cyber crime like by updating the computer, by choosing strong passwords, by protecting computer with security software, Be Social-Media Savvy.

Sundar Pichai [5]state the security and identity management systems that can operate in mobile and cloud environments, enable greater use of behavioral analytics, and take advantage of smart device capabilities to protect users and data from hackers, fraudsters and cybercriminals.

Some of these technologies can unilaterally be employed by Wolf, G., Pfitzmann [3]. To use others, bilateral cooperation is needed, e.g. the cooperation of both communication partners. For some, trilateral cooperation is required. One example is that of legally binding digital signatures, which not only require the cooperation of the (at least two) communicating parties, but additionally at least one trusted third party for the certification of public keys. For other technologies, multilateral cooperation between a large numbers of independent parties may even be necessary. We will use this distinction to structure a short overview of what is known about technology for security, providing pointers to the relevant literature.

Mostly the cyber attacker focus on data, they create alteration process, deletion process such type process over the data. To prevent this type of crime the Hemraj Saini et al. [4] suggest Data Interception techniques. In this case an attacker monitors data streams & try to gather information. This attack data collected may be the end goal of the attack. This attack usually involves sniffing network traffic, but may include observing other types of data streams. This differs from attacks that collect more qualitative information, such as communication volume, not explicitly communicated via a data stream. For such type of attacks the Data Increption Techniques are used.

III. OVERVIEW OF CYBER CRIME

Cyber space is a very broad term and it includes all things which are related with cyber crimes and laws such as Computers, networks, hardware, software, data storage devices, internet, E-mails. The term cyber crime means criminal activity over the Computer or Computer Network. The criminal activity includes everything from electronic cracking to denial of service attacks. The Cyber Crime consists

of unauthorized access to Computer Systems data alteration, data destruction or create nuance over the social network. The cyber crimes are categorized in different parts on the basis of their criminal activities. The categorization of cyber crime is also called as variants in cyber crime. The few variants are Hacking, Cyber Stalking, Site Scripting, Vishing, Phishing, etc.

These variants are elaborated as follows-

Hacking: In this case initially Hacker creates the unauthorized access in the data stored by cracking the system. Hacking has included many different motivations and activities. Hackers are one uniform group with a single purpose. Generally anyone who engages in illegal computer activity without investigating or considering their motivations and goals is known as Hackers.

Site Scripting: Site Scripting allows code injection by malicious web users into the web pages viewed by other users. Such type of criminal activity found in web application. Examples of such code include HTML code and client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls.

Cyber Stalking: Cyber stalking is used to stalk someone by using the Internet or other electronic means. This term is used interchangeably with online harassment and online abuse. Stalking generally involves harassing such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages.

Vishing: Vishing is the criminal activity of using social engineering and Voice over Internet Protocol to gain access to private .personal and financial information from the public for the purpose of financial reward**.** Vishing exploits the public trust in telephone services, which have traditionally terminated in physical locations which are known to the telephone company. Vishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.

Phishing: Phishing is just one of the many frauds on the Internet, trying to fool people in ordered to grab their money from their online accounts. In this case they request them to enter their username, password or other personal information.

But we should not much worry in case of above problems because they have yet not been sorted out up to the satisfactory level. Many works have been done to solve the problems.

IV. IMPACT OF CYBER CRIME

Impact on Economic / Finances

A.R. Raghavan and Latha Parthiban [7] state that the Information Communication Technology has revolutionalized different aspects of human life and has made our lives simpler. It has been applied in different industries and has made business processes simpler by sorting, summarizing, coding, and customizing the processes. However, ICT has brought unintended consequences in form of different cybercrimes. Cybercrimes have affected different industries and banking sector is one of them which have witnessed different forms of cybercrimes like ATM frauds, Phishing, identity theft, Denial of Service.

Impact on Private Sector / Industry

Bryan Watkins [9] explains the Impact of Cyber Attacks on the Private Sectors. He suggests that Companies are turning to insurance as financial protection against the inevitable threat of attacks. While cyber insurance often covers the cost to repair systems after security breaches as well as regulatory fees, most policies have exceptions limiting the scope of coverage to exclude loss of stolen intellectual property or business intelligence. Still, cyber insurance is a booming business.

Impact on Government

Cyber terrorism is one distinct kind of crime in this category explain by the Singh et al [10]. The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to threaten the citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website. The Parliament attack in Delhi and the recent Mumbai attack fall under this category. India had enacted its first Cyber Law through IT Act 2000. It has been amended and now in 2008 the revised version is under implementation.

Impact of Cyber Crime over Teenager:

The term Cyber Bullying states the details idea about the Cyber Crime over Teenagers. Cyber Bullying is a fear when person receives threats, negative comments or negative pictures or comments from other person. This is all done through mainly via online. Cyber Bulling can be done through chatting, instant messaging etc. Where website like Facebook, Orkut, Twitter user are more affected from Cyber Bullying. In my analysis generally feared person can reach a limit of depression, humiliation and threatens. Through this analysis we come to analyze that if person Bulled online he or she may be depressed up to the level of self harming

CONCLUSIONS

This research not only reviews the area of cyber crimes but also explains the impacts over the different levels of the society. This will help to the each person or society to secure all the online information which is not safe due to cyber crimes. The understanding of the behavior of cyber criminals and impacts of cyber crimes on society will help to find out the sufficient means to overcome the situation. The way to overcome these crimes can be classified into different categories just like Cyber Laws, Cyber Education and Ethics of Cyber, Policy making etc. All the above ways to handle cyber crimes either are having very less significant work. This lack of work requires to improve the existing work or to introduce new technology for controlling the cyber crimes.

REFERENCES

1. Vineet Kandpal and R. K. Singh; "Latest Face of Cybercrime and Its Prevention In India"; in International Journal of Basic and Applied Sciences Vol. 2. No. 4. 2013. Pp. 150-156
2. Source: Sundar Pichai, speaking at a Google breakfast briefing, July 2013
3. Wolf, G., Pfitzmann, A. Properties of protection goals and their integration into a user interface; Computer Networks 32, 2000, pp. 685-699.
4. Hemraj Saini, Yerra Shankar Rao, T.C.Panda, "Cyber-Crimes and their Impacts: A Review" in International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 2,Mar-Apr 2012, pp.202-209
5. Goldenberg, J, Libai, B, Muller, E: Talk of the network: a complex systems look at the underlying process of word-of-mouth. Marketing Letters. 12(3), 211–223.
6. Metaxas, PT, Mustafaraj, E, Gayo-Avello, D: How (not) to predict elections. In: Proceedings of the 3rd International Conference on Privacy, Security, Risk and Trust (PASSAT) and the 3rd International Conference on Social Computing (SocialCom), (2011)

7. A.R. Raghavan and Latha Parthiban International Journal of Current Research and Academic Review ISSN: 2347-3215 Volume-2 Number 2 (February-2014) pp.173-178
8. Thomas, K, Grier, C, Paxson, V: Adapting social spam infrastructure for political censorship. In: Proceedings of the 5th USENIX Conference on Large-Scale Exploits and Emergent Threats (LEET), (2012)
9. Bryan Watkins;, "The Impact of Cyber Attacks on the Private Sector ", August 2014
10. Singh et al., International Journal of Advanced Research in Computer Science and Software Engineering 3(5), May - 2013, pp. 997-1002