International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Understanding Cyber Crimes: Impacts on Society and Future Trends in Online Threats

Manav Madhav Kalyankar

En. no.2211271070077
BSc - FS (Sem - 5) Batch - A

Abstract: ***In the current era of online processing, maximum of the information is online and prone to cyber threats. 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. 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 etc. Restriction of cyber crimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society. Therefore, the current manuscript provides the understanding of cyber crimes and their impacts over society with the future trends of cyber crimes.***

Keywords: Cyber Attacks, Cyber Crimes, Potential Economic Impact, Consumer trust, National Security

1. Introduction

Current era is too fast to utilize the time factor to improve the performance factor. It is only possible due the use of Internet. The term Internet can be defined as the collection of millions of computers that provide a network of electronic connections between the computers. There are millions of computers connected to the internet. Everyone appreciates the use of Internet but there is another side of the coin that is cyber crime by the use of Internet. The term cyber crime can be defined as an act committed or omitted in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction. Other words represents the cyber crime as ―Criminal activity directly related to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored or on - line data, or sabotage of equipment and data. ‖ [1]. The Internet space or cyber space is growing very fast and as the cyber crimes. Some of the kinds of Cyber - criminals are mentioned as below.

- Crackers: These individuals are intent on causing loss to satisfy some antisocial motives or just for fun. Many computer virus creators and distributors fall into this category.
- Hackers: These individuals explore others' computer systems for education, out of curiosity, or to compete with their peers. They may be attempting to gain the use of a more powerful computer, gain respect from fellow hackers, build a reputation, or gain acceptance as an expert without formal education.
- Pranksters: These individuals perpetrate tricks on others. They generally do not intend any particular or long-lasting harm.
- Career criminals: These individuals earn part or all of their income from crime, although they Malcontents, addicts, and irrational and incompetent people: "These individuals extend from the mentally ill do notnecessarily engage in crime as a full - time occupation.
- Cyber terrorists: There are many forms of cyber terrorism. Sometimes it's a rather smart hacker breaking into a government website.

1.1. Data Crime

a) Data Interception
An attacker monitors data streams to or from a target in order to gather information. This attack may be undertaken to gather information to support a later attack or the 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, such as radio. In most varieties of this attack, the attacker is passive and simply observes regular communication, however in some variants the attacker may attempt to initiate the establishment of a data stream or influence the nature of the data transmitted. However, in all variants of this attack, and distinguishing this attack from other data collection methods, the attacker is not the intended recipient of the data stream.

b) Data modification

c) Data theft

1.2 Network Crime

a) Network Interferences
Network Interfering with the functioning of a computer Network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing Network data.

b) Network Sabotage
'Network Sabotage' or incompetent managers trying to do the jobs of the people they normally are in charge of? It could be the above alone, or a combination of things.

1.3 Access Crime

a) Unauthorized Access
"Unauthorized Access" is an insider‘s view of the computer cracker underground. The filming took place all across the United States, Holland and Germany. "Unauthorized Access" looks at the personalities behind the computers screens and aims to separate the media hype of the 'outlaw hacker' from the reality [7].

b) Virus dissemination

2. Impacts of Cyber - Crime

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. Organized crime groups are using the Internet for major fraud and theft activities. There are trends indicating organized crime involvement in white - collar crime. As criminals move away from traditional methods, internet- based crime is becoming more prevalent. Internet - based stock fraud has earned criminals millions per year leading to loss to investors, making it a lucrative area for such crime.

2.1 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. Further analysis of this growing problem found that 69 percent of adults that are online have been victims of cyber crime resulting in 1 million cyber crime victims a day. Many people have the attitude that cyber crime is a fact of doing business online! [18]. 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

2.2 Impact on Market Value

The economic impact of security breaches is of interest to companies trying to decide where to place their information security budget as well as for insurance companies‘ that provide cyber - risk policies [19]. For example, a ruling in favor of Ingram. Micro stated that ―physical damage is not restricted to physical destruction or harm of computer circuitry but includes loss of use and functionality‖ [20]. This new and evolving view of damage becomes even more important as many firms rely on information systems in general and the Internet in particular to conduct their business. This precedent may force many insurance companies to compensate businesses for damage caused by hacker attacks and other security breaches.

3. Future Trends

One of the biggest concerns is what if there is a hack into the critical systems in government, companies, financial institutions etc. This could lead to malware in critical systems leading to data loss, misuse or even killing the critical systems. Since the communication flow is easy via the internet, the crime organizations might merge and cooperate even more than they are currently. Memory Scraping Will Become More Common in the coming time. This has been around for a long time, but is more aggressively targeting data such as credit card records, passwords, PIN's, keys, as of late. The reason they are successful is that they get around PCI/GLBA/HIPAA/ETC security requirements that data must be encrypted while in transit and at rest. Data in transit is decrypted on the system and often stored in memory during the lifetime of a process, or at least during a decryption routine. Depending on how a process cleans up after itself, it may stay resident even after the fact.

4. Conclusion

This manuscript put its eye not only on the understanding of the cyber crimes but also explains the impacts over the different levels of the society. This will help to the community to secure all the online information critical organizations which are not safe due to such 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 broadly be classified into three categories: Cyber Laws (referred as Cyber laws), Education and Policy making. All the above ways to handle cyber crimes either are having very less significant work or having nothing in many of the countries. This lack of work requires to improve the existing work or to set new paradigms for controlling the cyber attacks.

References

[1] Shantosh Rout (2008), Network Interferences, Available at: http: //www.santoshraut. com/ forensic/cybercrime. htm, Visited: 28/01/2012
[2] Gordon, L. A. et al., 2003, A Framework for Using Insurance for Cyber - Risk Management, Communications of the ACM, 46 (3): 81 - 85.