A study on effect of Cyber attack on society

Archana Bhatt
Assistant Professor
Dr.Prenana Sharma
Assistant Professor
Chameli Devi group of Professional Studies
Indore, Madhya Pradesh

Abstract

In the current era of online processing, maximum of the information is online and prone to cyber threats. Whilst society is inventing and evolving, at the same time, criminals are deploying a remarkable adaptability in order to derive the greatest benefit from it.To avoid giving cybercriminals the initiative, it is important for those involved in the fight against cybercrime to try to anticipate qualitative and quantitative changes in its underlying elements so that they can adjust their methods appropriately. 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 crime. It is increasingly being used for pornography, gambling, trafficking in human organs and prohibited drugs, hacking, infringing copyright, terrorism, violating individual privacy, money laundering, fraud, software piracy.

Key Words*: - Internet, Hacking, Society*

Introduction

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. Cybercrime combines the term ‘crime’ with the root "cyber" from the word "cybernetic", from the Greek, ‘kubernân’, which means to lead or govern. Crime is a social and economic phenomenon and is as old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is “a legal wrong that can be followed by criminal proceedings which may result into punishment.” A crime may be said to be any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequences.

The expanding reach of computers and the internet has made it easier for people to keep in touch across long distances and collaborate for purposes related to business, education and culture among others. Any technology is capable of beneficial uses as well as misuse. It is the job of the legal system and regulatory agencies to keep pace with the same and ensure that newer technologies do not become tools of exploitation and harassment.

Types of Cyber Crimes

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.

b.Data Modification Privacy of communications is essential to ensure that data cannot be modified or viewed in transit. Distributed environments bring with them the possibility that a malicious third party can perpetrate a computer crime by tampering with data as it moves between sites.

c. Data Theft Term used to describe when information is illegally copied or taken from a business or other individual. Commonly, this information is user information such as passwords, social security numbers, credit card information, other personal information, or other confidential corporate information.

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

b.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 (3).

c. Virus Dissemination Malicious software that attaches itself to other software. (Virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are examples of malicious software that destroys the system of the victim.

1.4. Related Crimes

a. Aiding and Abetting Cyber Crimes There are three elements to most aiding and abetting charges against an individual. The first is that another person committed the crime. Second, the individual being charged had knowledge of the crime or the principals' intent. Third, the individual provided some form of assistance to the principal.

Crime is referred to as an "accessory after the fact".

b. Computer-Related Forgery and Fraud: Computer forgery and computer-related fraud constitute computer related offenses.

c. Content Related Crimes : Cyber sex, unsolicited commercial communications, cyber defamation and cyber threats are included under content-related offenses.

Impacts of Cyber-Crime

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. Police departments across the nation validate that they have received an increasing number of such crimes reported in recent years. This is in sync with the national trend resulting from increased computer use, online business, and geeky sophisticated criminals.

3.1 Perception of the Impact of Cybercrime

The impact of cybercrime is hard to identify. Yet, there is an increase in the development of information technology and the exploitation of vulnerabilities among cybercriminals, a gap between lawful and corrupt countries, and a paradox related to technological developments and breakthroughs. It is always worthwhile to remember that technology itself is neutral. However, its use can be described as negative or positive. This is especially true in cryptography, used for securing transactions and data interchange as well as to secure communications covering illegal activities and the establishment of evidence.

3.2 Negative Developments with regard to Cybercrime

Expected developments, which may have a negative impact on cybercrime, render little distinction between work life and private life, using for example the difficulty of locating information for a company and Web applications with cloud computing, targeted stealth malware, and more generally, the massive use of new technologies, including mobile and wireless technologies, and a careless exposure to social engineering, social networks, and mobile downloads carried out less securely than in the past.

3.3 Positive Developments with regard to Cybercrime

Security measures based on these same technologies could have a positive impact. Security is central to the problem and must be based on policies and be strictly enforced. It will be a major challenge with cloud computing, due to the complexity of where data is stored and the numerous jurisdictions involved, major risks associated with governance and territoriality

Specific computer crimes

Malware: Malware is malicious software deliberately created and specifically designed to damage, disrupt or destroy network services, computer data and software.

There are several types:

Computer virus

Program which can copy itself and surreptitiously infect another computer often via shared media such as a floppy disk, CD, thumb drive, shared directory, etc. Viruses are always embedded within another file or program.

Worm : self-reproducing program which propagates via the network

Trojan horse: program which purports to do one thing, but secretly does something else; example: free screen saver which installs a backdoor.

Root kit : set of programs designed to allow an adversary to surreptitiously gain full control of a targeted system while avoiding detection and resisting removal, with the emphasis being on evading detection and removal.

Botne : set of compromised computers ("bots" or "zombies") under the unified command and control of a "botmaster;" commands are sent to bots via a command and control channel.

Spyware: assorted privacy –invading /browser-perverting programs

Spam

Spam, or the unsolicited sending of bulk email for commercial purposes, is unlawful to varying degrees. As applied to email, specific anti-spam laws are relatively new, however limits on unsolicited electronic communication have existed in some forms for some time. Spam, or the unsolicited sending of bulk email for commercial purposes, is unlawful to varying degrees. Spam originating in India accounted for one percent of all spam originating in the top 25 spam-producing countries making India the eighteenth ranked country worldwide for originating spam

Impact on Society of Ethical Hacking

Hackers are having very impact on the society. They are attracting more and younger generation. Though ethical hacking is not bad but it is also very important to know that what exactly ethical hackers are doing for the interest of society. Now a day's internet has become the gateway for any computer to connect to the entire world, which also makes it vulnerable to attacks from the hackers across the world.

A .Impact on Education

It is really very hard to teach students hacking. Students are more interested to learn new technique. As far as global technological knowledge is concerned it is very important to give the latest knowledge to students in the field of IT and other related areas. "A very big problem with undergraduate students to teach this approach that a teacher is effectively providing a loaded gun to them "(4) There is one another a very big problem with undergraduate students that they actually don't understand the importance and effectiveness of the hacking, but yes definitely they want to apply it either for good or bad purpose.

B.Impact On Business

All business transactions are done electronically or I can say In today' world no business is without the use of IT With the growth of Internet there are number of shopping and auctions websites those are influencing customers and selling their goods online. These sites are giving very good rewards and other discounts as well. It is very easy for an ethical hacker to buy number of goods and can avoid paying the amount because they know that they can easily do it. It is very unfortunate that some skilled professionals use their skills and ability to harm the society by finding vulnerabilities in their company's system, attacking them, creating virus programs, making code for not to accept the payment for the desired service.

C. Impact on Work Place and Its Security

We know that today's world every data of the company is in the electronic form. Ethical hacker can easily take this data and manipulate it according to his need and requirement. At the workplace it is very important to maintain its security and safety Ethical hacker can steal all the information and personal data related to employees. He may even make information inaccurate as well. Ethical hacker is in the company as the name of security person in IT but we will never come to know what exactly he can do. He may write the virus code or even allow the virus code to enter into the company's server to harm it.

D. Impact On Technology

There are certain tools available through which anybody can easily get the information related to any system either local or remote. Ethical hacker can easily get the IP addresses of any system and may harm it. For ethical hackers there are many tools available in the global market to help them to do their job effectively. NMap is the effective tool which is available on internet to download and use, it help an ethical hacker to find open ports of the different systems. Acunetix is the tool which tests for web applications vulnerabilities and it is available on internet for unethical hacker it is very easy to use and get the information. Hackers may use them for criminal intentions whereas ethical hackers will use them for the organizations benefits and to identify the weaknesses and flaws in the network security.

Cyber Crimes and The Nature of Evidence

The nature of evidence in the real world and the virtual world is different. This disparity is conspicuous in all the stages of evidence detection, gathering, storage and exhibition before the court. The critical part is that all the investigation authorities that are responsible right from the stage of collection of the evidence to the presentation of the evidence before the court must understand the distinguishing attributes of the evidence so that they can preserve the evidence collected by them. In this regard the role of the judiciary also becomes vital as the judiciary must also be in the position to appreciate the computer evidence presented before them. Contrary to the real world crimes where any tangible evidence in the form of finger prints, weapon of crime, blood stain marks etc can be traced, in the virtual world such traces become very difficult to find. The science of computer forensics is gaining significance in the investigation departments, corporate world, government departments etc. Let us understand some of the challenges that are involved in the process of cyber evidence detection, gathering, storage and exhibition before the court.

Conclusion

As the Cyber Crime is growing in wide scale and becoming a global issue. Regardless of regional and national boundaries researchers are working together to find out all possible solutions. Cross Domain Solutions suggest both the parties to follow protocols and standards The Educational Institutes can play vital role to make a strong ethical base by including such subjects as compulsory ones. Government may do frequent checking on Cyber Community for illegal services and face them to strictly follow the standards

References

1 Wow Essay (2009), Top Lycos Networks, Available at: http://www.wowessays.com/ dbase/ab2/ nyr90.shtml, Visited: 28/01/2012.

2 Oracle (2003), Security Overviews, Available at: http://docs.oracle.com/cd/B13789_01/ network.101/ b10777/overview.htm, Visited: 28/01/2012.

3. IMDb (2012), Unauthorized Attacks, Available at: http://www.imdb.com/title/tt0373414/, Visited: 28/01/2012

4 Tom Wulf, 2003, “Teaching Ethics in Undergraduate Network”, Consortium for Computing Sciences in College, Vol 19 Issue 1, 2-3.