CYBERCRIME

Megha Yadav

Guru Gobind Singh Indraprastha University, New Delhi

INTRODUCTION

Cybercrime is a crime that involves a computer and a network. The computer may have been used in the commission of the crime. Cybercrimes are responsible for the interruption of normal computer functions and has been known to cause the downfall of many companies and personal entities. Cybercrimes may be defined as: offences that are committed against individual or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet and mobile phones. Cybercrime may threaten a person or a nations security and financial health. Issues surrounding these are hacking, copyright, infringement, unwarranted mass surveillance, sextortion, child pornography, and child grooming.

These crimes create a negative stigma that use of technology is dangerous because practically anyone can access one's private information for a price. Technology continues to promote to ease our daily lives; however, there are dangers of using technology. One of the main danger of using technology is the threat of cybercrimes. The advantages of technology and the internet have led more criminals to use cyberspace to commit crimes. The threat of cybercrimes is increasing as globalization continues to spread across the world. While the impact of globalization has led to amazing, new discoveries throughout the world, internet connectivity has also made cybercrimes easier. Cybercrimes creates an overwhelming task for law enforcement bureaus since they are extremely technological crimes. Law enforcement organizations must have individuals trained in computer disciplines and computer forensics in order to accurately investigate computer crimes.

The purpose of this paper is to educate individuals who don't know what are cybercrimes and its importance in growing technological advance throughout society. Understanding the threat of cybercrime is a very pertinent issue because technology holds a great impact on our society as a whole.

CAUSES & METHODS OF PERPETRATION OF CYBERCRIMES

There are many ways or means where cybercrimes can occur. Here are a few causes and methods of how cybercrimes can be committed. Hacking, theft of information contained in electronic form, email bombing, data diddling, attacks, denial of service attack, virus and web jacking.

- **Hacking**: In other word can be referred to as the unauthorized access to any computer system or network. This method can occur if computer hardware and software had any weakness which can be infiltrated if such hardware or software has a lack in patching, security control, configuration or poor password choice.
- **Theft of Information**: This type of method occurs when information stored in computer system are infiltrated and are altered or physically being seized via hard disks; removable storage media or other virtual medium.
- **Email Bombing**: This is another form of internet misuse where individuals directs a mass numbers of mail to the victim, or an address in attempt to overflow the mailbox, which may be an individual or a company or even mail servers there by ultimately resulting into crashing. There are two methods of perpetrating an email bomb which include mass mailing and list linking.
- **Data Diddling**: Is the changing of data before or during an intrusion into the computer system. This kind of an occurrence involves moving raw data just before a computer can process it and then altering it back after the processing is completed.
- **Denial of Service Attack**: Is basically where a computer system becomes unavailable to its authorize end user. This form of attack generally relates to computer networks where the computer of the victim is submerged with more requests than it can handle which in turn causing the pc to crash. E.g. love bug arises, which affected virus 5% of the computers around the world.
- **Virus/ Worms Attacks**: Viruses are programs that can embed themselves to any file. The program then copies itself and spreads to other computers on a network which they affect anything on them, either by changing or erasing it. However, worms are not like viruses, they do not need the host to attach themselves to but make useful copies of them and do this constantly till they consume up all the available space on a computer's memory. E.g. love bug virus which affected at least 5% of the computers around the world.
- **Web Jacking**: This is where the hacker obtains access and can control website of another person, where he or she can destroy or alter the information. This type of method was MIT (Ministry of Information Technology) was hacked by the Pakistani.

THEFT CRIMES AND CYBER TERRORISM

Cyber terrorism may be defined to be where the deliberate use of disrupting activities, or the risk thereof, via virtual machine, with the purpose to further public, political, spiritual, radical or to threaten any person in continuance of such purposes. Theft crimes can include Credit/debit card fraud, identity theft, non-delivery of goods and services.

- Credit/debit card fraud is the unlawful use of a credit/debit card to falsely attain money or belongings. Credit/debit card numbers can be stolen from leaky websites, or can be obtained in an identity theft scheme.
- Identity theft: This is when someone seizes another's individual information without his or her awareness to commit theft or fraudulency. Typically, the victim is led to

believe they are revealing sensitive private data to genuine business, occasionally as a response to an email to modernize billing or membership information etc.

- Non-delivery of goods and services: goods and services that were acquired by individuals online those were never sent.

CYBERCRIME AGAINST CORPORATIONS

Companies have the same risk of being attacked by different cybercrimes. Such crimes include Business schemes, counterfeit check method.

- **Business schemes**: Normally includes crimes stated above in theft crimes but more specifically freight forwarding and counterfeit check schemes. This is where an ad for help is posted by the imposter on one of popular internet job search sites via the internet. The respondents have to fill out an application where give sensitive private data such as their date of birth or social security number about themselves. The impostor than pays the freight forwarder with a counterfeit check containing a substantial excess amount. The excess is wired back to the impostor, usually in a foreign country, before the fraud is exposed.
- **Counterfeit check method**: This is where a fake cashier cheque or corporate check is used to pay for goods or services. Most often these checks are made out of larger amount of money than the buying price asking for. The victims are asked to deposit the check and return the excess amount, usually done wire transfer, to a foreign country due to banks may issue monies from a cashier check before the check usually clears. The victim now believes the check has cleared and wires the money as indicated. One example of this scam is purchasing of automobiles.

LAWS GOVERNING CYBERCRIMES

In this section of this paper we'll discusses laws and legislation that governs cybercrime in the United States and within other countries worldwide. This section will highlight some laws and let people know some of the laws that are out there to protect them and some of the amendments to these laws to keep up with the different advancements in technology.

In the United States

In the United States, the legislation concerning cybercrimes differs from state to states. In other words, each state has their own way of dealing with different types of cybercrimes being committed on a daily basis. Congress combats cybercrimes by enacting several laws such as The Computer Fraud and abuse act of 1984 (CFAA). At the time such it was difficult for federal law enforcers to use such legislation to indict anyone because of the difficulty of writing such an act. The act however requires major proof that personnel suspect has or have accessed computers without authorization which in turn can be a major limitation. In 1994, the act was altered again to meet new complications that arose such as malicious codes which at the time were bugs, viruses, worms and other programs that were intended to harm or modify data on a computer.

In 2002, cyber security enhancement act was passed. The act helped law agencies to increase punishments which were set out in the CFFA which in turn means harsher punishments for individuals who willingly committed computer crimes in the end result of even bodily injuries etc. those punishments can range from 5 to 20 years, or even life imprisonment.

CRIMINAL JUSTICE RESPONSE TO CYBERCRIME

The criminal justice system response to cybercrime is the advent and the development of the field of digital forensics, which has its roots in data recovery methods. That is, digital forensics has evolved into a field of complex, controlled procedures that allow for near real-time analysis leading to accurate feedback. Such analysis allows individuals in criminal justice to track the changes and key issues that are pertinent to good investigation of cybercrime. Another method that criminal justice uses to combat cybercrime is through education of the public. This includes publishing important tips for reducing victimization. For instance, the National White Collar's Center (NW3C) 2007 report suggested several ways that various forms of cybercrime may be reduced. For example, cyberstalking may be reduced by following these steps:

- Use a free email account for news group/mailing lists, chat rooms instant messages(IMS), emails from strangers, message boards, filling out forms, and other online activities.
- Don't give your primary email address to anyone you do not know or trust.
- Instruct children to never give out their real name, age, address, or phone number over the internet without your permission.
- Don't provide your credit card number or other information to access or subscribe to a website with which you are not familiar.
- Monitor/observe news groups, mailing lists, and chat rooms before "speaking" or posting messages.
- When you do participate online, be careful- type only what you would say to someone's face.
- When communicating online, don't reveal personal things about yourself until you really and truly know the other person.
- The first instinct when someone attack you online may be to defend yourself- don't this is how most online harassment situations begin.

Remember, if your bank or credit card company needs you to contact it, there are telephone numbers and web site information on your statement. You do not have to click on unsolicited emails to contact the company.

POTENTIAL IMPACT OF THE RESEARCH

This research will make constant progress possible or even give us victory in the fight against cybercrime. It will also inculcate innovative and inductive thinking and it promotes the development of security consciousness in organization.

The outcome of this research will have its special significance in solving various information security related problems of government agencies, the business community and individuals alike. When all these are achieved, we will end up making our cyber space a safer place for business transaction, there by indirectly affecting the economy. The internet will be a better and safer place for transaction and users will be better informed of security tips for the safety of their transactions.