Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Cyber Crime – A Threat to Persons, Property,Government and Societies

Er. Harpreet Singh Dalla, Ms. Geeta
HOD, Department of CSE & IT
Patiala Institute of Engineering & Technology for Women,
Patiala, India.

Abstract- In the present day world, India has witnessed an unprecedented index of Cyber crimes whether they pertain to Trojan attacks, salami attacks, e-mail bombing, DOS attacks, information theft, or the most common offence of hacking. Despite technological measures being adopted by corporate organizations and individuals, we have witnessed that the frequency of cyber crimes has increased over the last decade. Since users of computer system and internet are increasing worldwide in large number day by day, where it is easy to access any information easily within a few seconds by using internet which is the medium for huge information and a large base of communications around the world. Certain precautionary measures should be taken by all of us while using the internet which will assist in challenging this major threat Cyber Crime. In this paper, i have discussed various categories of cyber crime and cyber crime as a threat to person, property, government and society. In this paper I have suggested various preventive measures to be taken to snub the cyber crime.

Keywords: Cyber crime. Computer crime, hacking, cyber fraud, Prevention of cyber crime.

I. Introduction

In the present day world, India has witnessed an huge increase in Cyber crimes whether they pertain to Trojan attacks, salami attacks, e-mail bombing, DOS attacks, information theft, or the most common offence of hacking the data or system to commit crime. Despite technological measures being adopted by corporate organizations and individuals, we have witnessed that the frequency of cyber crimes has increased over the last decade. Cyber crime refers to the act of performing a criminal act using computer or cyberspace (the Internet network), as the communication vehicle. Though there is no technical definition by any statutory body for Cyber crime, it is broadly defined by the Computer Crime Research Center as - "Crimes committed on the internet using the computer either as a tool or a targeted victim." All types of cyber crimes involve both the computer and the person behind it as victims; it just depends on which of the two is the main target. Cyber crime could include anything as simple as downloading illegal music files to stealing millions of dollars from online bank accounts. Cyber crime could also include non-monetary offenses, such as creating and distributing small or large programs written by programmers called viruses on other computers or posting confidential business information on the Internet. An important form of cyber crime is identity theft, in which criminals use the Internet to steal personal information from other users. Various types of social networking sites are used for this purpose to find the identity of interested peoples. There are two ways this is done - phishing and harming, both methods lure users to fake websites, where they are asked to enter personal information. This includes login information, such as usernames and passwords, phone numbers, addresses, credit card numbers, bank account numbers, and other information criminals can use to "steal" another person's identity.

II. History

The first recorded cyber crime took place in the year 1820 which is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage. In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This was the first recorded cyber crime.

III. Manifestations

Basically cyber crimes can be understood by considering two categories, defined for the purpose of understanding as Type I and Type II cyber crime.

Type I cyber crime has the following properties:

It is generally a single event from the perspective of the victim. For example, the victim unknowingly downloads or installs a Trojan horse which installs a keystroke logger on his or her machine. Alternatively, the victim might receive an e-mail containing what claims to be a link to a known entity, but in reality it is a link to a hostile website. There are large number of keylogger soft wares are available to commit this crime.

It is often facilitated by crime ware programs such as keystroke loggers, viruses, root kits or Trojan horses.

Some types of flaws or vulnerabilities in software products often provide the foothold for the attacker. For example, criminals controlling a website may take advantage of vulnerability in a Web browser to place a Trojan horse on the victim's computer. Examples of this type of cybercrime include but are not limited to phishing, theft or manipulation of data or services via hacking or viruses, identity theft, and bank or e-commerce fraud.

Type II cybe crimes, at the other end of the spectrum, includes, but is not limited to activities such as computer related frauds, fake antivirus, cyber-stalking and harassment, child predation, extortion, travel scam, fake escrow scams, blackmail, stock market manipulation, complex corporate espionage, and planning or carrying out terrorist activities. The properties of Type II cyber crime are:

- It is generally an on-going series of events, involving repeated interactions with the target. For example, the target is contacted in a chat room by someone who, over time, attempts to establish a relationship. Eventually, the criminal exploits the relationship to commit a crime. Or, members of a terrorist cell or criminal organization may use hidden messages to communicate in a public forum to plan activities or discuss money laundering locations.
- It is generally facilitated by programs that do not fit into the classification of crimeware. For example, conversations may take place using IM (Instant Messaging). Clients or files may be transferred using FTP.

IV. Cyber Crime In India

Reliable sources report that during the year 2005, 179 cases were registered under the I.T. Act as compared to 68 cases during the previous year, reporting the significant increase of 163% in 2005 over 2004. (Source: Karnika Seth - Cyber lawyer & Consultant practicing in the Supreme Court of India and Delhi High Court)

Some of the cases are:

- The BPO, Mphasis Ltd. case of data theft
- The DPS MMS case
- Pranav Mitra's email spoofing fraud

V. Some Professions Giving Birth To Cyber Crimes

There are three kinds of professionals in the cyberspace:

1. IT or Tech Professionals

Since Cyber Crime is all about computers and Networks (Internet), many types of IT & Technology professionals are quite prominently active in the same, which include but are not restricted to:

- Network Engineers
- Cyber Security Software Professionals
- Cyber Forensic Experts
- IT Governance Professionals
- Certified Internet Security Auditors
- Ethical Hackers

2. Cyber Law Experts

Cyber Law has become a multidisciplinary approach and hence specialization in handling cyber crimes is required. Cyber law experts handle:

- Patent and Patent Infringements or other Business Cyber crimes
- Cyber Security for Identity thefts and Credit Cards and other Financial transactions
- General Cyber Law
- Online Payment Frauds
- Copyright Infringement of software, music and video.

3. Cyber Law Implementation Professionals

Many agencies play a role in cyber law implementation, which include the e-Governance agencies, law and enforcement agencies, cybercrime research cells and cyber forensic labs. Each of these would have a different category of professionals.

VI. Categories Of Cyber Crime

Cybercrimes can be basically divided into four major categories:

1. Cyber crimes against persons.

Cyber crimes committed against persons include various crimes like transmission of child-pornography, cyber porn, harassment of a person using a computer such as through e-mail, fake escrow scams. The trafficking, distribution, posting,

and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important Cyber crimes known today. The potential harm of such a crime to humanity can hardly be explained. Cyber-harassment is a distinct Cyber crime. Various kinds of harassment can and do occur in cyberspace, or through the use of cyberspace. Different types of harassment can be sexual, racial, religious, or other. Persons perpetuating such harassment are also guilty of cyber crimes.

Cyber harassment as a crime also brings us to another related area of violation of privacy of citizens. Violation of privacy of online citizens is a Cyber crime of a grave nature. No one likes any other person invading the invaluable and extremely touchy area of his or her own privacy which the medium of internet grants to the citizen. There are certain offences which affect the personality of individuals can be defined as:

Harassment via E-Mails: This is very common type of harassment through sending letters, attachments of files & folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Facebook, Twitter, Orkut etc. increasing day by day.

Cyber-Stalking: It is expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.

Defamation: It involves any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.

Hacking: It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programs. Hackers usually hacks telecommunication and mobile network.

Cracking: It is act of breaking into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.

E-Mail Spoofing: A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates.

SMS Spoofing: Spoofing is a blocking through spam which means the unwanted uninvited messages. Here a offender steals identity of another person in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is very serious cyber crime against any individual.

Carding: It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account. There is always unauthorized use of ATM cards in this type of cyber crimes.

Cheating & Fraud: It means the person who is doing the act of cyber crime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.

Child Pornography: In this cyber crime defaulters create, distribute, or access materials that sexually exploit underage children.

Assault by Threat: It refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

2. Cyber crimes against property.

The second category of Cyber-crimes is that of Cyber crimes against all forms of property. These crimes include computer vandalism (destruction of others' property) and transmission of harmful viruses or programs. A Mumbai-based upstart engineering company lost a say and much money in the business when the rival company, an industry major, stole the technical database from their computers with the help of a corporate cyber spy software. There are certain offences which affects persons property which are as follows:

Intellectual Property Crimes: Intellectual property consists of a bunch of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an crime. The most common type of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.

Cyber Squatting: It involves two persons claiming for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. For example two similar names i.e. www.yahoo.com and www.yahhoo.com.

Cyber Vandalism: Vandalism means deliberately damaging property of another. Thus cyber vandalism means destroying or damaging the data or information stored in computer when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral or a device attached to the computer.

Hacking Computer System: Hackers attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity there will be loss of data as well as computer system. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company. As in April, 2013 MMM India attacked by hackers.

Transmitting Virus: Viruses are programs written by programmers that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They mainly affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computer system of the individuals.

Cyber Trespass: It means to access someone's computer or network without the right authorization of the owner and disturb, alter, misuse, or damage data or system by using wireless internet connection.

Internet Time Thefts: Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. You can identify time theft if your Internet time has to be recharged often, despite infrequent usage.

3. Cyber crimes against government.

The third category of Cyber-crimes relates to Cyber crimes against Government. Cyber terrorism is one distinct kind of crime in this category. 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.

From the International Cyber Law Expert

Pauline Reich is an American lawyer and professor at Waseda University of Law in Tokyo, Japan. As hailed by the Japan Times, she is 'A pioneer in the field of cyber crime.' She spoke to SME WORLD on the present state of cyber crime in India and other countries and what are the systems in place for dealing with the menace.

When the European Convention drafted the Cyber Crime Convention, no exact definition of cyber crime was provided. Every country has its own way of defining cyber crime, which is peculiar to its own socio-cultural situations. For instance, in India defamation is a significant and rampant form of cyber crime.

The UN is strongly trying to put in place a global mechanism to improve awareness as well as to implement and install effective security measures for cyber crime.

The Council of Europe Cyber Crime Convention is also in place. Countries have to bring their own national laws upto the international benchmark and then ratify the convention.

4. Cybercrimes Against Society at large:

An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. These offences include:

Child Pornography: In this act there is use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity.

Cyber Trafficking: It involves trafficking in drugs, human beings, arms weapons etc. which affects large number of persons. Trafficking in the cybercrime is also a gravest crime.

Online Gambling: Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. In India a lot of betting and gambling is done on the name of cricket through computer and internet. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.

Financial Crimes: This type of offence is common as there is huge growth in the users of networking sites and phone networking where culprit will try to attack by sending bogus mails or messages through internet. Ex: Using credit cards by obtaining password illegally.

Forgery: It means to deceive large number of persons by sending threatening mails as online business transactions are becoming the habitual need of today's life style.

VII. Major Threats Of Cyber Crime In The Current Scenario

Well at present, cases such as credit card thefts and online money-laundering are on the rise. Cyber crime has also exposed the impending hazards of e-banking. Zenophobia, hate-mail cases and cyber-terrorism are the most pronounced aspects of cyber crime across countries. Fake escrow scams, online infringement of music, videos and software also having big impact in cyber crime. Well, as far as India is concerned, I don't see very effective laws in place to address such cases. However, I appreciate the amendment made in the IT Act, 2000. When the IT Act was passed way back in 2000, the Act majorly addressed issues related to e-commerce.

VIII. Impact Of Cyber Crime On Businesses

As all the businesses, all over the world are increasingly operating in the online mode because most of their work being done through websites, hence all sectors are equally vulnerable to cyber crime. Cyber Crimes always affects the companies of any size because almost all the companies gain an online presence and take advantage of the rapid gains in the technology but greater attention to be given to its security risks.However, I would say that SMEs in the IT industry are the greatest stake holders. Piracy and copy right protection are the major threats.

IX. Action To Be Taken By Companies And Entrepreneurs On Cyber Criminals

Well, the most important step would be to educate people on how to protect themselves (privacy) from being intrusively invaded by cyber criminals. Secondly the employees need to be trained on how to protect their work.

As for the HR department, the task is to conduct thorough pre-employment checks. In the modern cyber technology world it is very much necessary to regulate cyber crimes and most importantly cyber law should be made stricter in the case of cyber terrorism and hackers.

X. Major Deterrents For The Police And The Companies So For As Detecting Cyber Crimes

Companies in India do not want to be publicized for the wrong reasons. If ever they are in trouble, they try their best to sort it out through own in-house security system.

As far as the police are concerned they are usually reluctant to take up cyber crime cases as investigation is highly labour-intensive and expensive.

XI. Prevention Of Cyber Crime

Prevention is always better than cure. It is always better to take certain precautions while working on the net. One should make them a part of his cyber life.

Sailesh Kumar Zarkar, technical advisor and network security consultant to the Mumbai Police Cyber crime Cell, advocates the 5P mantra for online security: Precaution, Prevention, Protection, Preservation and Perseverance.

- Identification of exposures through education will assist responsible companies and firms to meet these challenges.
- One should avoid disclosing any personal information to strangers, the person whom they don't know, via e-mail or while chatting or any social networking site.
- One must avoid sending any photograph to strangers by online as misusing or modification of photograph incidents increasing day by day.
- An update Anti-virus software to guard against virus attacks should be used by all the netizens and should also keep back up volumes so that one may not suffer data loss in case of virus contamination.
- A person should never send his credit card number or debit card number to any site that is not secured, to guard against frauds.
- It is always the parents who have to keep a watch on the sites that their children are accessing, to prevent any kind of harassment or depravation in children.
- Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt some policy for preventing cyber crimes as number of internet users are growing day by day.
- Web servers running public sites must be physically separately protected from internal corporate network.
- It is better to use a security programs by the body corporate to control information on sites.
- Strict statutory laws need to be passed by the Legislatures keeping in mind the interest of netizens.
- IT department should pass certain guidelines and notifications for the protection of computer system and should also bring out with some more strict laws to breakdown the criminal activities relating to cyberspace.
- As Cyber Crime is the major threat to all the countries worldwide, certain steps should be taken at the international level for preventing the cybercrime.
- A complete justice must be provided to the victims of cyber crimes by way of compensatory remedy and offenders to be punished with highest type of punishment so that it will anticipate the criminals of cyber crime.

XII. Conclusion

In conclusion, computer crime does have a drastic effect on the world in which we live. It affects every person no matter where they are from. It is ironic that those who in secret break into computers across the world for enjoyment have been labeled as deviance. Many hackers view the Internet as public space for everyone and do not see their actions as criminal. Hackers are as old as the Internet and many have been instrumental in making the Internet what it is now. In my view point hacking and computer crime will be with us for as long as we have the Internet. It is our role to keep the balance between what is a crime and what is done for pure enjoyment. Luckily, the government is making an effort to control the Internet. Yet, true control over the Internet is impossible, because the reasons the Internet was created. This is why families and the institution of education of is needed, parents need to let their children know what is okay to do on the computer and what is not and to educate them on the repercussions of their actions should they choose to become part of the subculture of hackers.

In finishing this paper, the true nature of what computer crime will include in the future is unknown. What was criminal yesterday may not be a crime the next day because advances in computers may not allow it. Passwords might be replaced for more secure forms of security like biometric security. Most of the recorded computer crimes cases in most organization involve more than individual and virtually all computer crime cases known so far are committed by employer of the organization. Criminals have also adapted the advancements of computer technology to further their own illegal activities. Without question, law enforcement must be better prepared to deal with many aspects of computer-related crimes and the techno-criminals who commit them. This article is not meant to suggest that programmers or computer users are fraudulent people or criminal but rather to expose us to the computer-related crime and provides ways to prevent them.

Since users of computer system and internet are increasing worldwide in large number day by day, where it is easy to access any information easily within a few seconds by using internet which is the medium for huge information and a large base of

communications around the world. Certain precautionary measures should be taken by all of us while using the internet which will assist in challenging this major threat Cyber Crime.

References

[1] Communications Fraud Control Association. 2011 global fraud loss survey. Available: http://www.cfca.org/fraudlosssurvey/, 2011.

[2] F. Lorrie, editor. "*Proceedings of the Anti-Phishing Working Groups*", 2nd Annual eCrime Researchers Summit 2007, Pittsburgh, Pennsylvania, USA, October 4–5, 2007, vol. 269 of ACM International Conference Proceeding Series. ACM, 2007.

[3] I. Henry, "*Machine learning to classify fraudulent websites*". 3rd Year Project Report, Computer Laboratory, University of Cambridge, 2012.

[4] Microsoft Inc. Microsoft security intelligence report, volume 9, 2010. Available: http://www.microsoft.com/security/sir/.

[5] Neilson Ratings. (2011). Top ten global web parent companies, home and work. Retrieved February 24, 2012.

[6] N. Leontiadis, T. Moore, and N. Christin. "*Measuring and analyzing search-redirection attacks in the illicit online prescription drug trade*". In Proceedings of USENIX Security 2011, San Francisco, CA, August 2011.

[7] Phil Williams, Organized Crime and Cybercrime: Synergies, Trends, and Responses, Retrieved December 5, 2006 from Available: http:// www.pitt.edu/~rcss/toc.html.

[8] Steel.C. (2006), Windows Forensics: The Field Guide for Corporate Computer Investigations, Wiley.

