Episteme: an online interdisciplinary, multidisciplinary & multi-cultural journal

Bharat College of Commerce, Badlapur, MMR, India

Volume 3, Issue 4 **March 2015**

CYBER SECURITY: A GLOBAL CONCERN

By Veena Nirgudkar

Abstract

Information technology has spread throughout the world. As the user of cyberspace grows increasingly diverse and the range of online interaction expands, there is expansion in the cyber crimes i.e. breach of online contracts, perpetration of online torts and crimes etc. Due to these consequences there was need to adopt a strict law by the cyber space authority to regulate criminal activities relating to cyber and to provide better administration of justice to the victim of cyber crime. In the modern cyber technology world it is very much necessary to regulate cybercrimes.

It can also include 'denial of services' and viruses attacks preventing regular traffic from reaching your site. Cyber crimes are not limited to outsiders except in case of viruses and with respect to security related cyber crimes that usually done by the employees of particular company who can easily access the password and data storage of the company for their benefits. Cyber offence addresses all types of criminal behaviour and abuse. It includes identity theft, computer data, frauds, forgery, hacking, stalking, and unauthorized' use, tampering of system and data and alike.

Keywords: Cyber crime, Digital world, Netizens

Introduction

In the era of cyber world as the usage of computers became more popular, there was expansion in the growth of technology as well, and the term 'Cyber' became more familiar to the people. The evolution of Information Technology (IT) gave birth to the cyber space wherein internet provides equal opportunities to all the people to access any information, data storage, analyse etc. with the use of high technology. Due to increase in the number of netizens, misuse of technology in the cyberspace was clutching up which gave birth to cyber crimes at the

domestic and international level as well.

Today's age, is age of information. Digital infrastructure is taking all aspects of mode society rapidly. Internet has erased the physical boundaries and created world wide information system. This worldwide infrastructure has created a problem, of information security. Cyber crimes have posed a threat across the globe, which can cause colossal losses as also cause harm to peace and harmony to human life.

Definition & Concept

Though the word Crime carries its general meaning as "a legal wrong that can be followed by criminal proceedings which may result into punishment" whereas Cyber Crime may be "unlawful acts wherein the computer is either a tool or target or both".

Cyber, Crimes Actually Means: It could be hackers vandalizing your site, viewing, confidential information, stealing trade secrets or intellectual property with the use of internet.

It can also include 'denial of services' and viruses attacks preventing regular traffic from reaching your site. Cyber crimes are not limited to outsiders except in case of viruses and with respect to security related cyber crimes that usually done by the employees of particular company who can easily access the password and data storage of the company for their benefits. Cyber crimes also includes criminal activities done with the use of computers which further perpetuates crimes i.e. financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail, spoofing, forgery, cyber defamation, cyber stalking, unauthorized access to Computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system etc.

Cyber offence addresses all types of crirninal behavior and abuse. It includes identity theft, computer data, frauds, forgery, hacking, stalking, and unauthorized' use, tampering of system and data and alike.

The world 1st computer specific law was enacted in the year 1970 by the German State of Hesse in the form of 'Data Protection Act, 1970' with the advancement of cyber technology. With the emergence of technology the misuse of technology has also expanded to its optimum level and then there arises a need of strict statutory laws to regulate the criminal activities in

the cyber world and to protect technological advancement system. It is under these circumstances Indian parliament passed its "INFORMATION TECHNOLOGY ACT, 2000" on 17th oct to have its exhaustive law to deal with the technology in the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cyber crimes.

Overview

Recent Survey has revealed that out of 100 companies 72% claimed to be victims of cyber crimes and 8% were unaware of information security breaches and 45% have experienced information security breaches. The report further said that less than 5% computer crimes were reported to law enforcement agencies.

Techniques

If we analyze the cyber crimes we find that it a collection of various techniques used to manipulate human behaviour and divulge confidential information or computer system access. These techniques are based on specific attributes of human decision making basis. These basis are also called as, 'BUGS' in human hardware. The attackers exploit them in various combinations and never comes face to face with victim following are some the popular crimes and techniques:-

1. **Pretexting**:– In this act the attacker creates a scenario to preserve a target to redress information or to perform an act and is mostly done over a Telephone or email or message. It involves a Ire• based on some prior research or set up or use of known information such as impersonation, date of birth, email-Id, pin number, last paid bill.

2. **Phishing**: - Here the phisher fraudulently obtains information of victim. Typically attacker send email which appears legitimate business, a bank or credit card company requesting verification of information and warning of some dire consequences. It usually contains a link to fraudulent web pages that has company logo and content looking legal. It has form requesting everything from home address to ATM / Pin number.

It is also known as brand spoofing or carding. It impairs the confidential information for identity theft. It is absolutely safe for attackers to rob the cash from the account of the victim as it leaves almost no proof.

Recently phishing has extended in social networking sites such as facebook, tweeter, and orkut targeting the private communications such as instant messaging, Wi-Fi, and Bluetooth is another soft target as elders using cyber space as they are unaware of the dangers in the cyber space.

3. **I V R Phone Phishing**: - This technique means interactive voice response system used by attackers who creates a copy of bank or business IVR system. The victim is asked to call on a toll free number of the bank for information verification. The system rejects the log in of victim continuously victim continuously so that the victim enters "Pin' or "Password' multiple times and reveals more passwords and information. Sometimes the attackers poses as 'Customer Care Agent' and gather more information by using typical commands and records e. g. 'Press. 1 - To change password' and / or 'Press .2 - To speak to customer care' etc.

4. **Trojan or gimmies**:- Gimmies exploits a curious or greedy victim. It could be a email virus which comes as an email attachment which promises, something' Cool' or 'Sexy' or anti - virus or system upgrade to the victim or even a cool gossip about fellow colleague. The victim opens the attachment without any thought a d it becomes active and then attacker get access for i side attacks, hiding inside the software.

5. **Road Apple**: - It uses physical media floppies, C D, or flash drives, which are infected with virus and when greedy curious victim inserts these into system it gives easy access to the attackers.

Latest survey has revealed that 90% of office workers gave researchers important passwords and information for cheap lures such as choclates, pen etc. A cybercriminal is sophisticated, educated, white collared, techno savvy persons and cast, creed, religion, age has no bar. He has an advantage that he never comes face to face with victim, therefore, he is faceless. He could be anybody a student, a technocrat, amateur or a hard core criminal too.

Classifications Of Cyber Crimes: Cyber Crimes which are growing day by day, it is very difficult to find out what is actually a cybercrime and what is the conventional crime so to come out of this• confusion, cybercrimes can be classified under different categories which are as follows:

1. **Cyber Crimes against Persons:**

There are certain offences which affect the personality of individuals can be defined as:

- Harassment via E-Mails:
- Cyber-Stalking:
- Dissemination of Obscene Material:
- Defamation:
- Hacking:
- Cracking:
- E-Mail Spoofing:
- SMS Spoofing:
- Carding:
- Cheating &Fraud:
- Child Pornography:
- Assault by Threat:

2**. Crimes against Persons Property:**

As there is rapid growth in the international trade where businesses and consumers are increasingly using computers to create, transmit and to store information in the electronic form instead of traditional paper documents. There are certain offences which affects persons property which are as follows:

Intellectual Property Crimes: Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form 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:
- Cyber Vandalism:
- Hacking Computer System:
- Transmitting Virus:
- Cyber Trespass:

- Internet Time Thefts

3. **Cybercrimes against Government:**

There are certain offences done by group of persons intending to threaten the international governments by using internet facilities. It includes:

- Cyber Terrorism:
- Cyber Warfare:
- Distribution of pirated software:
- Possession of Unauthorized Information:

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:
- Cyber Trafficking:
- Online Gambling:
- Financial Crimes:
- Forgery

Reason :

There are several reasons why statistics of cyber offences does not reveal real volume. The undisclosed cyber offences are referred by experts as dark figures following are some of the reasons: -

a. Cybercriminal is white collared, tech savvy persons and he never comes face to face with victims.

b. Operational speed and capacity makes it impossible to detect the cybercrime activity.

c. Many victims also have technical and legal ignorance in this regards.

d. May fear to report the offences for the fear of adverse publicity and loss of goodwill, confidence and embarrassment.

Following are the reasons, why people turn to such crimes:-

1. Revenge
2. Lure for and / or of money
3. Technical challenge
4. Plain Mischief and
5. Notorious promotion of ideology.

Like all other crimes cybercrime can be defeated through knowledge, common sense and few well-placed security measures. The road ahead is bumpy and full of challenges as under-

1. White collared criminal -
2. Ignorance of victims -
3. **Lack of technical personnel -**

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. In the modern cyber world cybercrimes is the major issue which is affecting individual as well as society at large too.

Need of Cyber Law

Information technology has spread throughout the world. The computer is used in each and every sector wherein cyberspace provides equal opportunities to all for economic growth and human development. As the user of cyberspace grows increasingly diverse and the range of online interaction expands, there is expansion in the cybercrimes i.e. breach of online contracts, perpetration of online torts and crimes etc. Due to these consequences there was need to adopt a strict law by the cyber space authority to regulate criminal activities relating to cyber and to provide better administration of justice to the victim of cybercrime. In the modern cyber technology world it is very much necessary to regulate cybercrimes and most importantly cyber law should be made stricter in the case of cyber terrorism and hackers.

Preventive Measures For CyberCrimes:

Prevention is always better than cure. A netizen should take certain precautions while operating) the internet and should follow certain preventive measures for cybercrimes which can be defined as the most obvious way to combat cyber offences is to stop them in the first place,

with improved technologies. It can be done at e layers-

a. The Consumer side,

b. The Server side,

c. The Enterprise side.

The enforcement agencies in India have to take consumer friendly and proactive monitoring, similar to European standards, which must include blacklisting operations, maintenance of an accessible system and deploying online phising radars, to track the online scans and frauds. Effective cyber security must ensure safety of digital infrastructure and date .integrity. It is important to stabilize consumer confidence. Lack of security could pose potential national threat.

Cybercrimes is not limited to any nation. It does not know any boundaries. It is a global concern hence; the key is to raise global awareness in this regard.

References:

1. Sanjay Mittal, Rahul Gupta: Detecting frauds in online Advertising system EC Web2008
2. Ghose Mamjuder Shuman Using data to help prevent fraud March 18 2008
3. www.legalserviceindia.com
4. www.indiantelevision.com
5. Report on Crime in India 2009 by National Crime Records Bureau Ministry of Home Affairs
6. Economic Times, June 5, 2013

Bio:

Veena Nirgudakar has been practicing law for last 31 years. She has also been teaching law for last 12 years. She has taught LLB degree programs 3 years as well as 5 years at D. Y. Patil Law college. She has been visiting faculty at various colleges such as MD collage Acharya College. Pragati College and Swami Vivekanand College. She is presently as HOD (Law) working at JVM's Mehta College, Navi Mumbai.

BCC-ISSN-2278-8794