REVIEW ON CYBER CRIME AND SECURITY

Pooja Aggarwal
papoojaaggarwal@gmail.com

Piyush Arora
piyush.arora357@gmail.com

Neha
isha.neha775@gmail.com

Poonam
poonamkumavat19@gmail.com

Dronacharya College of Engineering, Gurgaon

Abstract

The evolution of Information Technology gave birth to the cyber space where in internet provides equal opportunities all the people to access any information. Due to increase in the number of netizens, misuse of technology is increasing which leads to cyber crimes. The cyber crimes are basically undertaken by people in the age group from 13 to 25 years who all are well educated. Cyber crime refers to the unlawful acts where in the computer is either a tool or target or both. Cyber Security refers to mechanism by which computer-based equipments, information and services are protected from illegal and unauthorized access. The rules and regulations which are governing cyber space is known as Cyber Law which comprises of Information Technology Act 2000. There are cyber crime cells in every state to handle the cyber crime cases and to punish the netizens committing cyber crime. Cyber technology changes have been so rapid that there are laws which has some set of rules and guidelines that make the cyber activities legalized.

1. Introduction

Every human being is influenced by the information technology. The computer-based equipments, internet is used for betterment of life and to enhance speed of life. Due to increase in the use of technology, the crime is also increasing day-by-day. Cyber crime covers all forms of crime related to the computer networks [8]. Cyber crime is on the increase with criminals attempting several attacks worldwide [7]. The criminals are educated and technical experts having deep knowledge about the technology. There are several cyber crimes like hacking the ATM password, transferring all the money from victim's account to their accounts, pornography issues etc. In order to tackle these crimes, there is a need to implement some rules and regulations governing cyber space known as Cyber Law.

Information Technology Act 2000 includes several rules to deal with cyber offences. The severe punishment is provided to the criminals violating the cyber laws. These laws are also applicable to the persons residing outside India. Cyber security deals with the security of the cyber space and requires global cooperation. It involves protection of computer equipments, computer resources, information from unauthorized access and disclosure. The cyber law knowledge is the need for the persons working with computer networks to give rise to secured world with no fear of illegal works in cyber space. [9]

2. History of Cyber Crime

The first cyber crime took place in 1820. In 1820 Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom, a device which allowed the repetition of series of steps in weaving of special fabrics. This leads to fear in the minds of Jacquard employees and they committed the act of sabotage. This was the first recorded cyber crime.

In 1991 Kevin Poulsen was captured for selling military secrets. [3] In 1992 DarkAvenger released first polymorphic virus.

In 1997 FBI's National Computer Crime Squad reports 85% companies were hacked.

In 2001 Microsoft faced the attacks against domain name servers corrupting the Microsoft's websites. This was a Denial of Service (DoS) attack.

In 2007, a hacker exploits the eBay site by blocking the users and closing the sales. [10]

In 2008, Canadian porn site SlickCash pays $500K to Facebook after it tried to gain unauthorized access to Facebook's friend-finder functionality.

3. Types of Cyber Crime

1.1 Hacking

In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location. This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed. [3]

1.2 Theft

This crime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy. The FBI targets these websites and punishments are given to the criminals. [3]

1.3 Cyber Stalking

This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. The criminal follows the victim by sending the e-mails, entering the chat rooms frequently.
1.4 Denial of Service Attack
This is the act in which the criminal fills the victim's e-mail box by spam mails depriving him of the services he is entitled to access or provide. It is an attempt to make the network resources unavailable to its users.

1.5 Virus Dissemination
There are some malicious software that itself attaches to other software. The malicious software like virus, worm, trojan horse, time bomb, logic bomb completely destroys the system of the victim.

1.6 Software Piracy
Theft of software through illegal copying of genuine programs and distribution of the products intended for pass to the original. This can be done by end user copying, hard disk loading, counterfeiting, illegal downloads from the internet.

1.7 Pornography
The criminal harass the victim by blackmailing him/her by the illegal printed or visual material containing the explicit description of sexual organs or activity of the victim.

4. Types of Hackers
The cyber criminals are usually the educated people like engineers, MBA students, doctors etc who try to gain access of other's systems. These are:

1.1 Script Kiddies
These are wannabe hackers who want to be hacker or thins that they are but they lack the serious technical expertise. They are only able to hack the weakly secured systems. They can not cause any serious harm to the victims. [3]

1.2 Scammers
These send the fake e-mails to the victims like discount pharmaceuticals, fraud lottery prizes, time shares through which they are able to access the victim's system and corrupts it completely.

1.3 Hacker Groups
They work anonymously and hack computers for no criminal reasons. They are hired by organizations, government agencies etc. to test the security and handle the fraud cases.

1.4 Phishers
They requests confidential information over the internet under false pretenses in order to fraudulently obtain credit card numbers, passwords or other personal data. Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. [3]

1.5 Political/religious/commercial groups
They are not interested in financial gain. They develop malware for political ends. They try to gain access of the confidential information of the opponent groups. The Stuxnet worm which attacked Iran's Atomic Program of Its Nuclear Facilities was believed to be created by a foreign government.

1.6 Insiders
These attackers are considered to be the highest risks as they reside within the organization. They have the knowledge of all the details of an organization and easily attack the security of the company and corrupt the system. [3]

1.7 Advanced Persistent Threat (APT) Agents
This group is responsible for highly targeted attacks carried out by extremely organized state-sponsored groups. Their technical skills are deep and they have access to vast computing resources. It refers to a group, such as a government, with both the capability and the intent to persistently and effectively target a specific entity.

1.8 White Hat Hackers
They are referred to as ethical hackers who generally focus on securing the IT systems. The term white hat hacker is also often used to describe those who attempt to break into systems or networks in order to help the owners of the system by making them aware of security flaws. Many such people are employed by computer security companies; these professionals are sometimes called sneakers. Groups of these people are often called tiger teams. [3]

1.9 Black Hat Hackers
A black hat hacker is a person who compromises the security of a computer system without permission from an authorized party, typically with malicious intent. These hackers use their knowledge to exploit the systems for the private gain. They take advantage of break-in and results in destroying of secured files and steal the information. [3]

1.10 Grey Hat Hackers
A Grey Hat in the computer security community, refers to a skilled hacker who sometimes acts legally, sometimes in good will, and sometimes not. They are a hybrid between white and black hat hackers. They usually do not hack for personal gain or have malicious intentions, but may or may not occasionally commit crimes during the course of their technological exploits. [3]

5. Effects of Cyber Crime on Society
The cyber crime is an attack on information about people or groups which is very harmful as the criminals are mindful of the fact that all the organizations, common people, government agencies are reliant on the computers. [4]

1.1 Cyber Crime Against People
The criminal offers variety of fake promotions giving the people illusion of security thus forcing them to provide their personal information. The human trafficking of sexually explicit material which includes child pornography which is a major offence. The social networking sites and chat groups are also leads to serious cyber crimes. [5]
1.2 Cyber Crime Against Property

This includes the malicious software through websites, email or personal chats by which criminals can easily steal the information of other’s computer system. Theft of bandwidth that is gaining unauthorized access to an internet connection is also treated as a cyber crime.

1.3 Cyber Crime Against Business

This happens when the criminals hack the systems of business organizations as they store their confidential and sensitive data on the servers. They gain access to all the secured information of the company and transfer company’s funds to their accounts making the organization bankrupt.

1.4 Cyber Crime Against Government

The hackers hack the secured database of the government agency with the intention to use the sensitive information and are termed as “cyber terrorism”. Cyber crime is used to undermine the effectiveness of the government thus reducing the faith of the citizens in that government.

6. Cyber Law

Indian Cyber Law requires mainly of Information Technology Act. Cyber law or Internet law is a term that encapsulates the legal issues related to use of the Internet. "Computer law" is a third term which tends to relate to issues including both Internet law and the patent and copyright aspects of computer technology and software. It includes internet access and usage, privacy, freedom of expression, and jurisdiction.

The objective of IT Act 2000 is to provide legal recognition to electronic records and transactions carried out by way of electronic data interchange. The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures. [2]

There are few points which provide knowledge to the people on how to tackle cyber crimes:

- People need to be encouraged to report the matter to the law enforcement agencies with full confidence without the fear of being harassed.
- The knowledge of cyber law to the people will help them to tackle the fraud and imprison the criminals who try to harass them.

7. Cyber security

Cyber security refers to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals.

ISO 27001 (ISO27001) is the international Cyber security Standard that provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System. A fundamental role of ITU after the World Summit on the Information Society and the 2010 ITU Plenipotentiary Conference is to build the confidence and security in the use of Information and Communication Technologies. [6]

There are some prevention tips for cyber crime:

- Keep your infrastructure defense systems such as firewalls up to date.
- Make sure your computer is configured securely.
- Choose strong passwords for your systems, social networking sites, email boxes etc.
- Do not respond to the unfamiliar emails which demands for credit card details, personal information etc.
- Protect your computer with security software.
- Shield your personal information from strangers in the cyber space.

8. Cyber Security Standards

1.1 PAS 555

PAS 555 was released by the British Standards Institution (BSI) in 2013. PAS 555 is primarily intended as a framework for the governance of cyber security by allowing executives and senior management to compare the organization’s cyber security measures against the established descriptions at a high level. [8]

1.2 ISO/IEC 27001

ISO/IEC 27001 is the international standard for best practice information security management systems (ISMS). It includes specifications for protecting the system under the principles of confidentiality, integrity and availability. [1]

1.3 ISO/IEC 27032

ISO/IEC 27032 is the international standard focusing explicitly on cyber security. It includes the guidelines for protecting the system beyond the borders of organization and also against the cyber crimes that originate outside the cyber space.
1.4 CCM

The Cloud Security Alliance’s Cloud Control Matrix (CCM) is a set of controls designed to maximize the security of information for organizations that take advantage of cloud technologies.

1.5 ISO/IEC 27035

ISO/IEC 27035 is the international standard for incident management. This standard includes guidance for updating policies and processes to strengthen existing controls following analysis of the event and minimizing the risk that it recurs. [3]

1.6 ISO/IEC 27031

ISO/IEC 27031 is the international standard for ICT readiness for business continuity. This standard bridges the gap between the incident itself and general business continuity, and forms a key link in the chain of cyber resilience.

1.7 ISO/IEC 22301

ISO/IEC 22301 is the international standard for business continuity management systems (BCMS), and forms the final part of cyber resilience. This standard does not focus solely on the recovery from disasters, but also on maintaining access to and security of information, which is crucial when attempting to return to full, secure functionality.

9. Conclusion

In today’s modern era, the computer system and internet are increasing worldwide, thus making it easy for the cyber criminals to access any information by using their expertise. Cyber crime is defined as the unlawful acts where in the computer are either a tool or target or both. Cyber crime is a menace that has to be tackled effectively. The need is to create awareness among the people about the cyber space, various forms of cyber crimes and preventive measures. It is rightly said, “Prevention is better than cure”, thus it is advised to take precautions while operating on the internet. The internet users must adopt 5P mantra for their security, which is Precaution, Prevention, Protection, Preservation, Perseverance.

The IT Act is an articulation of all existing laws with “e” added to most of the provisions. Cyber Law knowledge must be known among the people working on the computer systems, computer networks and information communication technology.

References

[3] Information gained through the workshops conducted by i3indya Technologies

Ms. Pooja Aggarwal is currently pursuing BE from Dronacharya College of Engineering in Electronics and Communication Engg. She has good academic background and has interest in field of review/research. She has attended several workshops and seminars. Her areas of interest are Wireless Communication, Information technology, Mobile networks.

Mr. Piyush Arora is currently pursuing BE from Dronacharya College of Engineering in Electronics and Communication Engg. He has interest in field of review/research. He has attended several workshops and guest lectures. He also participated in international conference at IIT. His areas of interest are Wireless Communication, Data Communication, Embedded systems.

Ms. Neha is currently pursuing BE from Dronacharya College of Engineering in Electronics and Communication Engg. She has interest in field of review/research. She has attended several workshops and seminars. Her areas of interest are Wireless communication, Mobile ad hoc networks, Digital electronics.

Ms. Poonam is currently pursuing BE from Dronacharya College of Engineering in Electronics and Communication Engg. She has interest in field of review/research. She has attended several workshops and participated in several poster making competitions. Her areas of interest are Ad hoc networks, Antenna and wave propagation, Satellite communication.