Advances in Computational Research
ISSN: 0975-3273 & E-ISSN: 0975-9085, Volume 7, Issue 1, 2015, pp.-179-181.
Available online at http://www.bioinfopublication.org/jouarchive.php?opt=&jouid=BPJ0000187

CYBER CRIME INTENSIFICATION IN THE WORLD

GAIKWAD B.P.[1]* AND JADHAV M.E.[2]

[1]Department of CS and IT, Dr. Bababasaheb Ambedkar Marathwada University, Aurangabad - 431 001, MS, India.
[2]Department of CS and IT, Marathwada Institute of Technology, Aurangabad- 431 028, MS, India.
*Corresponding Author: Email- bharat.gaikwad08@gmail.com

Received: December 18, 2014; Revised: January 05, 2015; Accepted: January 15, 2015

Abstract- Internet crime is crime committed on the Internet. The cyber crime users are growing fast in the entire world and correspondingly the cyber criminals are also growing. The crime is performed by the user's cyber only when the connectivity through internet is made.

This paper takes a great privilege of introducing the concept of cyber crime followed by the reasons and types of cyber crime. Criminals give birth to crime and thus the cyber criminals are shown which are followed by the precautions and the acts and laws against cyber crime. The concluding part covers the world wide cases of cyber crime.

Keywords- cyber crime, hacking, cyber law

Citation: Gaikwad B.P. and Jadhav M.E. (2015) Cyber Crime Intensification in the World. Advances in Computational Research, ISSN: 0975-3273 & E-ISSN: 0975-9085, Volume 7, Issue 1, pp.-179-181.

Introduction

The evolution of the Internet, along came another revolution of crime where the perpetrators commit acts of crime and wrongdoing on the World Wide Web. Internet crime takes many faces and is committed in diverse fashions. The number of users and their diversity in their makeup has exposed the Internet to everyone. Some criminals in the Internet have grown up understanding this superhighway of information [2]. The unrestricted number of free Web sites; the Internet is undeniably open to exploitation. Known as cyber crimes, these activities involve the use of computers, the Internet, cyberspace and the World Wide Web.

The Cyber Crime has got different definitions as follows:

- Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber-crime.
- Cybercrime is a term used broadly to describe activity in which computers or networks are a tool, a target, or a place of criminal activity.

As the graph indicates the cases of cyber-crime progress in 20 counties increased. Thus it becomes necessary to understand each concept related to cyber crime and the steps being taken against cyber crime [1].

Types of Crime

Before evaluating the concept of cyber crime it is obvious that the concept of conventional crime be discussed and the points of similarity and deviance between both these forms may be discussed.

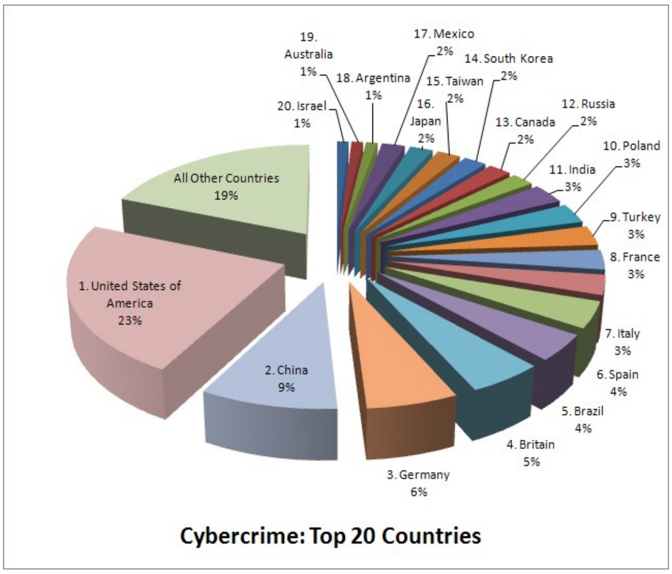

Fig. 1- Percentage of cyber-crime

Conventional Crime

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." The hallmark of criminality is that, it is breach of the criminal law. Per Lord Atkins "the criminal quality of an act cannot be discovered by reference to any standard but one: is the act prohibited with penal consequences". 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.

Cyber Crime

Cyber crime is the latest and perhaps the most complicated problem in the cyber world. "Cyber crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime"

Distinction Between Conventional and Cyber Crime

There is apparently no distinction between cyber and conventional crime. However on a deep introspection we may say that there exists a fine line of demarcation between the conventional and cyber crime, which is appreciable. The demarcation lies in the involvement of the medium in cases of cyber crime. The sine qua non for cyber crime is that there should be an involvement, at any stage, of the virtual cyber medium [9].

Reasons Behind Cyber Crime

The reasons for the vulnerability of computers may be said to be:

- Capacity to Store Data in Comparatively Small Space: The computer has unique characteristic of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium makes it much easier.
- Easy to Access: The problem encountered in guarding a computer system from unauthorised access is that there is every possibility of breach not due to human error but due to the complex technology.
- Loss of Evidence: Loss of evidence is a very common & obvious problem as all the data are routinely destroyed [2,3].

Cyber Criminals

The cyber criminals constitute of various groups/ category. This division may be justified on the basis of the object that they have in their mind. The following are the category of cyber criminals:

- Children and adolescents between the age group of 6 - 18 years: The simple reason for this type of delinquent behaviour pattern in children is seen mostly due to the inquisitiveness to know and explore the things.
- Organized Hackers: These kinds of hackers are mostly organised together to fulfil certain objective. The reason may be to fulfil their political bias, fundamentalism, etc.
- Professional Hackers / Crackers: Their work is motivated by the colour of money. These kinds of hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information [10].

Mode and Manner of Commiting Cyber Crime

Following are the different modes in which cyber crime takes place:

- Unauthorized access to computer systems or networks / Hacking: This kind of offence is normally referred as hacking in the generic sense. However the framers of the information technology act 2000 have no where used this term so to avoid any confusion we would not interchangeably use the word hacking for 'unauthorized access' as the latter has wide connotation.
- Theft of information contained in electronic form: This includes information stored in computer hard disks, removable storage media etc. Theft may be either by appropriating the data physically or by tampering them through the virtual medium.
- Email Bombing: This kind of activity refers to sending large numbers of mail to the victim, which may be an individual or a company or even mail servers there by ultimately resulting into crashing [3].
- Virus / Worm Attacks: Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves [6].

Fig. 2- Unlawful accessing info

Classification of Cyber Crimes

- The subject of cyber-crime may be broadly classified under the following three groups.

Against Individuals

- their person
- their property of an individual

Against Organization

- Government
- firm, company, group of individuals

Against Society at large

- Against Individuals
- Harassment via E-mails
- Cyber stalking
- Dissemination of obscene material
- Defamation
- Unauthorised control

Against Individual Property

- Computer vandalism
- Transmitting virus
- Netrespass

- Unauthorized access over computer system
- Intellectual Property crimes

Types of Cyber Crime

Following are the different types of cyber crime:

Communication in Furtherance of Criminal Conspiracy

Just as legitimate organizations in the private and public sectors rely upon information systems for communications and record keeping, so too are the activities of criminal organizations enhanced by technology. There is evidence of telecommunications equipment being used to facilitate organized drug trafficking, gambling, prostitution, money laundering, child pornography and trade in weapons.

Telecommunication Piracy

Digital technology permits perfect reproduction and easy dissemination of print, graphics, sound, and multimedia combinations. The temptation to reproduce copyrighted material for personal use, for sale at a lower price, or indeed, for free distribution, has proven irresistible to many.

Dissemination of Offensive Material

Content considered by some to be objectionable exists in abundance in cyberspace. This includes, among much else, sexually explicit materials, racist propaganda, and instructions for the fabrication of incendiary and explosive devices. Telecommunications systems can also be used for harassing, threatening or intrusive communications, from the traditional obscene telephone call to its contemporary manifestation in "cyber-stalking", in which persistent messages are sent to an unwilling recipient [4].

Electronic Funds Transfer Frauds

Electronic funds transfer systems have begun to proliferate, and so has the risk that such transactions may be intercepted and diverted. Valid credit card numbers can be intercepted electronically, as well as physically; the digital information stored on a card can be counterfeited [8].

Actions Against Cyber Crime

The Information Technology Act 2000 was passed and enforced on 17th May 2000.the preamble of this Act states its objective to legalise e-commerce and further amend the Indian Penal Code 1860, the Indian Evidence Act 1872, the Banker's Book Evidence Act1891 and the Reserve Bank of India Act 1934**.** The basic purpose to incorporate the changes in these Acts is to make them compatible with the Act of 2000 [2].

The Information Technology Act deals with the various cyber crimes in chapters IX & XI. The important sections are Ss. 43,65,66,67. Section 43 in particular deals with the unauthorised access, unauthorised downloading, virus attacks or any contaminant, causes damage, disruption, denial of access, interference with the service availed by a person[5,7].

Laws For Cyber Criminals

The Information Technology Act 2000 was undoubtedly a welcome step at a time when there was no legislation on this specialised field. The Act has however during its application has proved to be inadequate to a certain extent. The various loopholes in the Act are-

- The hurry in which the legislation was passed, without sufficient public debate, did not really serve the desired purpose.
- Cyber laws, in their very preamble and aim, state that they are targeted at aiding e-commerce, and are not meant to regulate cybercrime.
- Cyber torts.

Conclusion

The major reasons for e-criminal activity in computers are the theft of company documents, e-mail frauds, and unauthorized use of computers mostly breaking a username and password, harassment and stalking in cyberspace, releasing a malicious computer program that is virus and accessing the victim's computer via the Internet.I would conclude with a word of caution for the pro-legislation school that it should be kept in mind that the provisions of the cyber law are not made so stringent that it may retard the growth of the industry and prove to be counter-productive.

Conflicts of Interest: None declared.

References

[1] Schell B.H. & Clemens M. (2004) *Cybercrime: A Reference Handbook*.

[2] Wong A. & Yeung A. (2009) *Network Infrastructure Security*, Springer.

[3] Shukla D. & Thakur S. (2007) *Proceedings of National Conference on Network Security and Management*, 155-165.

[4] Eoghan C. (2004) *Digital evidence and computer crime, forensic science, computers and the internet*, 2nd ed., Academic press.

[5] Wang Y., Cannady J. & Rosenbluth J. (2005) *Computer Law and Security Report*, 21(2), 119-127.

[6] Singh S.P. & Maini A.R. (2012) International Journal of Computer Applications, 35, 459-468.

[7] Shukla D., Tiwari V. & Thakur S. (2010) *Journal of Global Research in Computer Science*, 1(4), 31-36.

[8] Gaikwad B.P. (2014) *International Journal of Innovative Research in Computer and Communication Engineering*, 2(5), 1-8.