Electronic International Interdisciplinary Research Journal (EIIRJ)

Impact Factor : 0.987

Reviewed Online Journal
(Bi-Monthly)
Mar-April ISSUES

Chief-Editor:

Ubale Amol Baban

www.aarhat.com

2015

INFORMATION COMMUNICATION TECHNOLOGY IS FULL OF BOONS BUT HAVING CURSE IN FORM OF CYBER CRIME

*Dr. Mukesh Yadav

Assistant Professor,

Government College of Education,

Bhiwani (Haryana)

Abstract:

Past two decades has been the witness of unprecedented progress in information, communication and related technologies in India. The society at large has reaped the benefits of the progress fuelled by the steep fall in computing and communication costs. But at the same time the world has listened to the ominous tunes of technological advancements. The gravity of cyber crime assumes more importance due to lack of awareness of Indian masses and the global nature of the crime. The paper reports the findings from the analysis of secondary data with regards to trends in cyber criminology.

Keyword*: Cyber Crime, Cyber Terrorism*

INTRODUCTION:

To date no single definition of cyber crime is there. Most commonly following definition is accepted in general:

"Any illegal offence involved, use of computer as the object of crime or the tool used to commit a crime"

Cyber crime spans not only state but national boundaries as well. At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cyber crime was broken into two categories and defined thus:

Firstly, cyber crime in a narrow sense is any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them. And, secondly cyber crime in a broader sense is any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession offering or distributing information by means of a computer system or network (Townsend, 2004)

Life is about a mix of good and evil. So is the internet. For all the good it does to us, Cyber crimes have its dark side too. Unlike conventional crimes though, there is no policeman

patrolling the information superhighway, leaving it open to everything from Trojan horses and Viruses to Cyber stalking, trademark counterfeiting and Cyber terrorism (Laura, 1996).

Cyber Crime is the latest type of crime which affects many people. It refers to the criminal activities taking place in computer or computer networks, intentionally access without permission, alters, damages, deletes and destroys the database available on the computer or network, and also includes access without permission on a database or programme of a computer in order to devise or execute any unlawful scheme or wrongfully control or obtain money, property or data. It poses the biggest challenge for the Police, Prosecutors and legislators. Crimes of this nature are usually indulged in by young teens, recreational computer programmers and persons having vested interest. Cyber crime in its most practiced form includes offences such as tampering with the source code of a programme, hacking into computer systems, publication of obscene information and misuse of licences and digital signatures. The problem is multifold as it covers the crime related to economy as well as other crimes such as pornography which has its basis in certain moral standards and uses parameters like indecency and obscenity

In many of the criminal cases the computer is never used as object or as a tool where the criminals use computer only for storing the data or for communication. Hence such type of crime is not considered to be cyber crime. With the adventure of Information communication and Technology the computer has speedup the processing of Information that in turn has improved the lift style of every one especially in case of public services. There is no doubt that the development of computing is skyrocketing. Most of the govt sectors and organizations are reliant on the internet. If the traditional style of working remains same then it is not surprising to say that they will be far behind in this competitive ICT age and will find themselves in the top list of outdated and perishing .Every picture has a proverbial dark side. So is the Computer. It has become the tool of and venue for the crime. Usually when any kind of crime happens there remains some major/minor tangible evidence that act as the evidentiary proof like Physical existence /finger prints But in case of crime committed over computer we try to understand those facts which does exist virtually but not in reality. The most challengeable situation is absence of Evidence or Evidence of absence.

Review of Literature

It is crystal clear that the ICT is playing catalytic role in our social life. The strength of ICT lies with its speed and the scale is used by unscrupulous elements to cause damage in the Cyber world. To elaborate the awareness about cyber crime In India some analysis has been performed. As per stastical data of Indiacrimestat.com (Visited frequently From August 2010 to

Feb 2011) on the basis of Ministry of Home Affairs, Govt of India under year wise tables were rearranged for total no. of cases registered(including cyber crime cases) and the number of persons arrested. It is clear that there is gradual increase in the no. of cyber crime cases, it being 70 in 2002 and increased to 288 in 2008 (about four times).

Further perusal of the data shows that from 2002 to 2008, about 65% of the Cyber Crimes committed are by the persons of age group between 18-30 years and 28% by the persons in the age group between 30-45 years This is one Cyber crime which threatens to undermine the growth of the younger generation as also leave irreparable scars and injury on the younger generation, if not controlled

Cyber crimes and attacks cost Indian companies Rs 58 lakh in revenue in 2009 and affected over 66% of Indian enterprises, according to a study by internet security providers, Symantec Corp. According to the findings on India in the research titled 2010 State of Enterprise Security, over and above these revenue losses, Indian enterprises also lost an average of Rs 94.56 lakh in organisation, customer and employee data, and an average of Rs 84.57 lakhs in productivity costs last year. Protecting information today is more challenging than ever. By putting in place a security blueprint that protects their infrastructure and information, enforces IT policies, and manages systems more efficiently, businesses can increase their competitive edge in todays information-driven world (www.symantec.com, 2010).

In the present era of rapid growth, information technology is encompassing all walks of life all over the world. These technological developments have made the transition for paper to paperless transaction possible. We are now creating new standards of speed, efficiency and, accuracy in communication, which has become key tools for boosting innovations, creativity and increasing overall productivity. Computers are extensively used in the storage of confidential data of political, social and economic or personal nature which are of immense benefit to the society. The use of Computers is increasingly spreading, and more and more users are connecting to the internet. The internet is a source for almost anybody to access, manipulate and destroy others information. The rapid development of the Internet and computer technology globally has also led to the growth of new forms of transnational crimes especially those which are internet related. These criminal activities directly relate to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored data, or sabotage of systems and data. Characteristic feature of these crimes are that these crimes are considered as illegal, unethical or unauthorized behaviour of people relating to the automatic

processing and transmission of data by the use of Computer Systems and Networks. These crimes have virtually no boundaries and may affect any country across the globe within a fraction of second.

In a day and age where everything from a microwave oven to nuclear plants run on computer and computer programmes, Cyber crimes has assumed a rather sinister implication. Life is about a mix of good and evil. So is the internet. For all the good it does to us, Cyber crimes have its dark side too. Unlike conventional crimes though, there is no policeman patrolling the information superhighway, leaving it open to everything from Trojan horses and Viruses to Cyber stalking, trademark counterfeiting and Cyber terrorism (Laura, 1996).

After discussing the above, it can be concluded that the Netizens are in a position to understand the things but not be concluded that all are well known about Cyber Crime. the true Netizen some times never knows that they have been involved in it or the online activity is one type of Cyber Crime. However the actual number of cyber crimes may continue to elude considering the fact that majority of the cases go unreported. The worst situation is because even honest users are clueless as to what is and is not Cyber Crime Indirectly it is contributing towards increase in Cyber Crime if not using the Security Protocols or reporting about the Cyber crime. The literature depicts that due to one or the other reason (a few are discussed below), the upcoming technological world is facing this crime:

- Computers can store unlimited amounts of data in small spaces
- The data can be easily accessed from any part of the world.
- Complexity of technology makes many of the reports undetectable.
- Human error like fail to implement the proper security protocols for their PCs
- One of the key elements that keeps most members of any society honest is fear of being caught — the deterrence factor. Cyberspace changes two of those rules. First, it offers the criminal an opportunity of attacking his victims from the remoteness of a different continent and secondly, the results of the crime are not immediately apparent.
- Need amendments in cyber laws and implementation of upgraded technology to combat cyber crimes

When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulation. Today, there are many disturbing things happening in cyberspace. Due to the anonymous nature of the Internet, it is possible to engage

into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence the need for Cyber laws in India Here comes the role of discussing this paper.

Objective:

The main objective of this study is:

1. To identify the frequency in cyber crime(s).
2. To study the awareness level of respondents for Cyber Crime(s).
3. To identify the contribution of technical factors in cyber crime(s)

Hypotheses

H1: There is no significant impact of technical factors to increase in cyber crime(s)

H2: There is no significant rate of reoccurrences of cyber crime(s).

H3: There is significant awareness in mass to be victim of cyber crime(s)

III. RESEARCH METHOD

Samples and Procedures

Forty respondents were given a brief lecture on cyber crime to be familiar by paper reading, text-book case and live case discussions. A Web-based questionnaire was set up specifically for this to stimulate the respondent's in-depth discussions. Ten teams were formed having four respondents in each. Each team had to respond to questions as per the questionnaire. Four respondents turned in an incomplete questionnaire and 36 were usable samples. Of the 36 respondents, 16 were from females.

Measures

To meet out the objectives of my study the following measure s have been taken in account:

1 .The questionnaire was designed to measure the variables

2 In terms of their knowledge Respondents were asked to tick againstoptions from list of questions in the table

3. The questionnaire was divided into three sections as per the objective

4 First section was having the tabular form of questions to measure the variable i.e. Frequency in cyber crime(s) consisting of 14 questions

Page 31

5. Second section was having the tabular form of questions to measure the variable i.e. awareness level of respondents for Cyber Crime(s). It consisted of 14 items in the form of questions to measure individual's awareness.

6   Third section was having the tabular form of questions to measure the variable i.e. contribution of technical factors in cyber crime(s). It consisted of 14 items in the form of questions to measure individual's awareness

Results and Discussion:

1.   Educating the population about cyber crime aiming to increase the number of reports and to improve the quality of information contained in those reports;

2.   Improving the channels communication with the victim with training on cyber crime for police officers who receive reports and developing tools to better collect, classify and co-relate the reports received from web pages and E-mail addresses;

3.   Increasing cyber patrolling activities, being more pro-active in monitoring internet access points like cyber cafes;

4.   Data or information is hold by internet service providers and telecom conference. For investigation of cyber crime the investigating agency must have contacts with them in the form of meetings/enquiries about cyber crime cases;

5.   No country have laws to force ISP and telecom companies to keep data for fixed period of time therefore, to trace the intangible cyber criminal activities the ISP must be forced legally to keep relevant information with it. Restricting the disclosure of such information only to law enforcement agencies conducting an investigation;

6.   This is the global threat due to its global access of internet, therefore, the countries must cooperate and fight together by :

    (i)   By searching and seizure of computers in the country if any request is received from another country.

    (ii)   By enforcing the law for deserving the information by ISP or telecom providers the country can deserve the computer data evidence at the request of another country subject to privacy issues.

Conclusion:

As we are living in 21st Century which is called as an InfoTech Age we should well aware about the various aspects of the information technology. The civilians used computers to secure their important data however at the same time the various security aspects should be taken into consideration; As many people are not well aware about the developments and growth in

communications, computers and the internet. The various concepts of electronic communication are unaware to the common man because of lack of knowledge, infrastructure and poverty. The common man should be literate so as to secure the information which is preserved in electronic form. The Government should also take various steps pertaining to the protection of data. The experts in Information Technology track the valuable information regarding defense and security of the nation. Such type of the act may threaten to the national and international peace. So as to protect the interest of nation we have to do research in such a field like cyber crime. Due to the emergence of computer networking and development in the area of internet and its frequent use in cyber crime, there are several issues and challenges that are addressed in the current research.

References*:*

www.symantec.com, 2010.

www.indiastatcrime.comAugust 2010-Feb2011

www.cybercrimelaw.net/content/history.html.

Laura E. Quarantiello, CYBER CRIME: HOW TO PROTECT YOURSELF FROM COMPUTER CRIMINALS. Tiare Publications, 1996.

John Townsend, CYBER CRIME, Raintree, 2004.

Kerr, Orin S. THE PROBLEM OF PERSPECTIVE IN INTERNET LAW, Georgetown Law Journal, 91, 357-405.

Dudeja V D, CRIMES IN CYBERSPACE- SCAMS AND FRAUDS (ISSUES AND REMEDIES) Commonwealth Publishers, New Delhi, 2003