International Journal of Innovative Research in Information Security (IJIRIS) ISSN: 2349-7009(P)
Issue 09, Volume 3 (December 2016) www.ijiris.com ISSN: 2349-7017(O)

CYBER CRIMES IN INDIA AND THE MECHANISM TO PREVENT THEM

K. Sambi Reddy.,
**ACTA –AP STATE PRESIDENT,*
Lecturer, Head of the Department, Department of Commerce, SS&N Degree College, Narasaraopet

Abstract*: 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. The objective of this paper is to discuss about the cyber crime and its categories, professions giving birth to cyber crimes and its impact on businesses and the preventive measures to be taken to control the cyber crime.

Keywords: Cyber crime, hacking, Cyber laws, Technology, Virus

INTRODUCTION: Technology has come to play a major role not only in the life of a consumer but also in the delivery of the services. The Government's push for digital India is a step towards ensuring access to Technology to every Indian. There is no doubt that today almost all service providers have made life easier by use of technology be it Banking, Insurance, E-Commerce etc. technology not only bridges the distance but also provides a better service to the consumers. With the rapid growth of Information technology in business, consumers are .now vulnerable to many risks. Electronic commerce has become a new form of strategic competition where the internet is used for communicating with customers and buying, selling products.

Consumers are doing online purchases and are defrauded by internet thieves sometimes. But the customers are not aware of the associate problems. Business methods and procedures are changing everyday but the laws regulating business are not changed at that frequency. Consumer protection may become a myth under these circumstances.

CYBER SPACE: The convergence of computer network and telecommunications facilitated by the digital technologies has given birth to a common space called 'cyberspace'. This cyberspace has become a platform for a galaxy of human activities which converge on the internet. The cyberspace has, in fact, become the most happening place today. Internet is increasingly being used for communication, commerce, advertising, banking, education, research and entertainment. There is hardly any human activity that is not touched by the internet. Therefore, Internet has something to offer to everybody and in the process it only increases and never diminishes. The *'cyber manthan'* has bestowed many gifts to humanity but they come with unexpected pitfalls. It has become a place to do all sort of activities which are prohibited by law. It is increasingly being used for pornography, gambling, trafficking in human organs and prohibited drugs, hacking, infringing copyright, terrorism, violating individual privacy, money laundering, fraud, software piracy and corporate espionage, to name a few.

CYBER CRIME: Cyber crime is not a matter of concern for India only but it is a global problem and therefore the world at large has to come forward to curb this menace. Further complicating cyber crime enforcement is the area of legal jurisdiction. Like pollution control legislation, one country cannot by itself effectively enact laws that comprehensively address the problem of internet crimes without cooperation from other nations. While the major international organizations, like the OECD and the G-8, are seriously discussing cooperative schemes, but many countries do not share the urgency to combat cyber crimes for many reasons, including different values concerning piracy or espionage or the need to address more pressing social problems. Though the issue of jurisdiction in cyberspace cannot be settled spontaneously, but still a global effort in this direction is the need of hour. India has witnessed a 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.

© 2014- 16, IJIRAE- All Rights Reserved

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.

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 is large number of keylogger software's are available to commit this crime. 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 CYBER 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 crime ware. For example, conversations may take place using IM (Instant Messaging). Clients or files may be transferred using FTP.*

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.

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.

© 2014- 16, IJIRAE- All Rights Reserved

- ***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 its 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.

- ***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.*
- ***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.*
- ***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.*
- ***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.*
- ***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.*

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.

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.*

© 2014- 16, IJIRAE- All Rights Reserved

- ***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.*

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.

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.

- *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.*
- *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.*

CONCLUSION:

Due to advancement of technology people apply their multiple or multi-label talent to misuse of technology and also make it harmful to other point of view. So this kind of crime not solved fully by establishing different law, also need to develop human morality, value and ethics in proper manner. 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. 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]. S. Hinde, "The law, cybercrime, risk assessment and cyber protection", Computers & Security, vol. 22, issue 2, pp. 90-95, February 2003.
[2]. Bequai, "A guide to cyber-crime investigations", Computers & Security, vol. 17, issue 7, pp.579-582, 1998.
[3]. www.cyberlawportal.com
[4]. Neilson Ratings. (2011). Top ten global web parent companies, home and work. Retrieved February 24, 2012.
[5]. 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.

© 2014- 16, IJIRAE- All Rights Reserved