CYBERCRIME: THE TRANSITION OF CRIME IN THE INFORMATION ERA

Shailza Dutt*

Dr. Suneyna*

Asha Chaudhary*

Abstract: *Computer crime also called as Cybercrime has increased in acuteness and occurrence in the current years and due to this, it has become a wide apprehension for companies, universities and organizations. Global governments, police departments and intelligence divisions have initiated to react.*

Society is becoming more dependent upon data and networks to police-based enforcement, with its genesis in real-world urbanization, does not and cannot defend society from criminals using computer technology. This paper gives data regarding operate our businesses, government, national defence and other critical functions. Cybercrime, which is fastly increasing in frequency and in acuteness, requires us to rethink how we should implement our criminal laws. The present model of reactive, cybercrime, its types, modes of cyber crime and security measures including stoppage to deal effectively with cybercrime. It shows a requirement for a timely review of existing approaches to fighting this new phenomenon of cybercrime in the information technology. Though it is impossible to remove Cyber Crime from the world but we can reduce it to a large amount by creating alertness in Society. We suggest a system of administrative regulation backed by criminal sanctions that will cater the incentives necessary to create a workable limiting to cybercrime.

Keywords: *Cyber Crime, Internet Crime, Law, Technology*

*Maharaja Sahimal Institute, Janakpuri, New Delhi

INTRODUCTION

From personal computers in the home used to follow checking accounts and keep household records in databases to large supercomputers that govern space missions and run the world's largest companies, computers have become commonplace. The total of individuals who have entrée to the data on those computers has spread as the communications industry has undergone a revolt in current years, and unrestrained admission to information presents a very actual risk in most business and some government information.

When the Internet was reputable, the founding fathers of the Internet barely had any tendency that the Internet could also be mishandled for criminal activities. Today, there are many alarming things happening in virtual space. Obviously, it was just a matter of time before criminals discovered the benefits of computers and make it rapidly possible to get patented information of financial institutions and other firms.

Because of the increasingly considerable role that computers play in modern life, there is a requirement to keep information on machines protected from altering, from unauthorized spreading, and from unlawful elimination.

EVOLUTION OF CYBER CRIME:

The first recorded cyber crime took place in the year 1820! That is not shocking considering the fact that the abacus, which is thought to be the initial form of a computer, has been around since 3500 B.C. in India, Japan and China. The epoch of modern computers, however, began with the analytical engine of Charles Babbage. In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, created the loom. This method allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a concern amongst Jacquard's employees that their old employment and livelihood were being warned. They committed acts of damage to discourage Jacquard from further usage of the new technology. This is the first noted cyber crime!

Cyber crime is a malevolent having its origin in the increasing reliance on computers in present life. In a day and epoch when everything from microwave ovens and refrigerators to nuclear power plants is being track on computers, cyber crime has supposed rather sinister repercusions. Many cyber crimes in the new past comprise the Citibank rip off. US $ 10 million were fraudulently transmitted out of the bank and into a bank account in Switzerland. A Russian hacker group led by Vladimir Kevin, a renowned hacker, executed the attack. The group negotiated the bank's security systems. Vladimir was allegedly using his office computer at AO Saturn, a computer firm in St. Petersburg, Russia, to halt into Citibank computers. He was finally captured on Heathrow airport on his way to Switzerland.

DEFINING CYBER CRIME

Defining cyber crimes, as "acts that are punishable by the Information Technology Act" would be unsuitable as the Indian Penal Code also covers many cyber crimes, such as email tricking and cyber transgression, sending threatening emails etc. A modest yet sturdy definition of cyber crime would be "unlawful acts wherein the computer is either a technique or a target or both".

OBJECTIVES OF CYBER CRIMES:

- To identify certain cyber crime divisions.
- To make misuse of data, systems and networks.
- To make changes in the confidential/secret information.

LITERATURE REVIEW:

- **David S. Wall.** Cambridge, UK **in his book "CYBERCRIME: THE TRANSFORMATION OF CRIME IN THE INFORMATION AGE"** addressed one significant dimension of the computer revolution: the advent of a wide range of crimes and harmful activities now carried out over the internet, and increasingly only made possible as a consequence of the existence of the internet, as well as the new and formidable challenges involved in controlling such crime.
- **Peter Grabosky,** of the Australian National University, most recently in **ELECTRONIC** CRIME (2007) – the present book is best described as a rather comprehensive survey

of what is presently known about cybercrime and its control. In this realm the term "presently" has to be emphasized in light of the exceptionally dynamic character of such crime, and the almost dizzying challenge of coming up with novel responses to each new technological break-through on the part of those engaged in cybercrime.

- Cyber-crime or computer crime is considered to be any crime that uses a computer and a computer network (**Matthews, 2010**). A basic definition describes cybercrime as a crime where computers have the possibility of playing an vital part (**Thomas and Loader, 2000**). The main factor in cyber-crime increase is the Internet. By use of Internet, cybercriminals often plea to images, codes or electronic communication in order to run malicious activities. Among the most vital types of Internet crimes we can mention: identity theft, financial theft, espionage, pornography, or copyright infringement.
- The cyber-crimes can be divided into two categories: the crimes where a computer network attacks other computers networks – e.g. a code or a virus used to disable a system, and, the second category, crimes where a computer network attacks a target population – e.g. identity theft, fraud, impositions (**Svensson, 2011**).
- Issues revolving around cyber-crime have become more and more complex. Computer criminal activities have grown in importance and institutions are more interested than ever in putting an end to these attacks. Progressions have been made in the development of new malware software, which can easily detect criminal behavior (**Balkin et al., 2007**). Moreover, high standard anti-virus systems are offered for free now in many countries at every purchase of a computer or an operating system.

MODES OF CYBER CRIMES:

Financial crimes

This would comprise cheating, credit card encroachments, money laundering etc. To cite a topical case, a website offered to sell Alphonso mangoes at a throwaway price. Mistrusting such a transaction, very few people responded to or supplied the website with their credit card numbers. These people were actually sent the Alphonso mangoes. The word about this website now amplified like wildfire. Many people from all over the country responded and well-ordered mangoes by providing their credit card numbers. The owners of what was later proven to be a fraud website then escaped taking the many credit card numbers and proceeded to spend big amounts of money much to the chagrin of the card keepers.

Cyber Pornography

This would comprise pornographic websites; pornographic magazines manufactured using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc). Recent Indian events hanging around cyber pornography include the Air Force Balbharati School case. A student of the Air Force Balbharati School, Delhi, was harassed by all his classmates for having a marked face. Tired of the cruel jokes, he decided to get back at his teasers. He skimmed photographs of his classmates and mentors, altered them with exposed photographs and put them up on a website that he uploaded on to a free web presenting service. It was only after the father of one of the class girls highlighted on the website challanged and lodged a complaint with the police that any action was booked.

In another incident, in Mumbai a Swiss couple would gather slum children and then would emphasise them to appear for not decent photographs. They would then upload these photographs to websites particularly planned for paedophiles. The Mumbai police arrested the duo for pornography.

Sale of Illegal Articles

This would comprise sale of narcotics, arms and wildlife etc., by posting data on websites, auction websites, and bulletin boards or 167 simply by using email E.g. Most of the auction sites even in India are supposed to be selling cocaine in the name of 'honey'.

Online Gambling

There are millions of websites; all introduced on servers overseas, that offer online. In fact, it is believed that most of these websites are really fronts for money laundering.

Intellectual Property Crimes

These include software piracy, copyright encroachment, trademarks violations, theft of computer source code etc.

Email Spoofing

A spoofed email is one that appears to start from one source but ultimately has been sent from another source. E.g. Priya has an e-mail address priya@asianlaws.org. Her enemy, Sameer spoofs her e-mail and sends indecent messages to all her associates. Since the e-mails appear to have originated from Priya, her friends could take offence and dealings could be spoiled for life.

Email spoofing can also cause monetary damage. In an American case, an adolescent made millions of dollars by spreading false information about specific companies whose shares he had short sold. This misinformation was increased by sending spoofed emails, allegedly from news agencies like Reuters, to share brokers and investors who were well-versed that the companies were doing very badly. Even after the truth came out the values of the shares did not go back to the earlier levels and manyinvestors lost a lot of money.

Forgery

Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be bogus using refined computers, printers and scanners. Outer many colleges from corner to corner India, one catches touts asking the sale of fake mark sheets or even certificates. These are made using computers, and big standard scanners and printers. In fact, this has increasing a booming business involving thousands of Rupees being given to student gangs in exchange for these fake but authentic looking certificates.

Cyber Defamation

This occurs when offence takes place with computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory data to all of that person's friends. In a current occurrence, Suman , a immature girl was about to be married to Sahi. She was actually pleased because despite it being an arranged relationship, she had liked the boy. He had appeared to be open-minded and nice. Then, one day when she met Sahi, he looked worried and even a little upset. He was not really concerned in talking to her. When asked he told her that, members of his family had been receiving e-mails that contained malicious things about Suman's character. Some of them spoke of dealings, which she have had in the past. He told her 168 that, his parents were justifiably very disappointed and were also considering breaking off the engagement. Fortunately, Sahi was able to succeed upon his parents and the other elders of his house to approach the police instead of blindly believing what was contained in the mails.

During investigation, it was shown that the person sending those e-mails was none other than Suman's stepfather. He had sent these e-mails so as to break up the relationship. The girl's relationship would have caused him to lose govern of her property of which he was the caretaker till she got married.

Another famous case of cyber defamation occurred in America. All peers and relatives of a lady were harassed with crude e-mail messages appearing to originate from her account. These mails were providing the lady in question a bad name among her groups. The lady was an activist against pornography. In reality, a group of people dissatisfied with her views and angry with her for contrasting them had decided to get back at her by using such underhanded methods. In accumulating to sending spoofed indecent e-mails they also put up websites about her, that basically slurred her character and sent e-mails to her family and friends containing matter defaming her.

Cyber Stalking

The Oxford dictionary defines stalking as "following quietly". Cyber stalking involves following a person's movements across the Internet by placing messages (sometimes threatening) on the bulletin boards frequented by the sufferer, the chat-rooms visited by the sufferer, constantly shelling the sufferer with emails etc.

FREQUENTLY USED CYBER CRIMES

Unlawful access to computer systems or networks

This activity is commonly referred to as hacking. The Indian law has however given a disimilar connotation to the term hacking, so we will not use the term "unlawful access" interchangeably with the term "hacking".

Pilfering of information contained in electronic form

This includes information stored in computer hard disks, removable storage media etc.

Email bombing

Email bombing refers to sending many emails to the sufferer resulting in the sufferer's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing. In one case, an immigrant who had been residing in Shimla, India for almost thirty years wanted to avail of a system started by the Shimla Housing Board to buy land at inferior rates. When he made an application it was rejected on the grounds that the 169 schemes was available only for people of India. He decided to take his avenge. Consequently he sent manymails to the Shimla Housing Board and repeatedly kept sending e-mails till their servers crashed.

Data Diddling

This type of an attack involves changing raw data just before it is processed by a computer and then altering it back after the processing is completed. Electricity Boards in India have been sufferers to data diddling programs inserted when private parties were computerizing their systems.

Salami Attacks

These attacks are used for the assignment of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely undetected. E.g. a bank executive inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 5 a month) from the account of every consumer. No account holder will probably notice this unofficial debit, but the bank employee will make a considerable amount of money every month. To cite an example, an employee of a bank in USA was dismissed from his job.

Discontented at having been supposedly mistreated by his employers the man first introduced a logic bomb into the bank's systems.

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 net. They usually affect the data on a computer, either by altering or removing it. Worms, unlike viruses do not need the host to attach themselves to. They merely make operational copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory. 170 The VBS_LOVELETTER virus (better known as the Love Bug or the ILOVEYOU virus) was reportedly written by a Filipino undergraduate.

Trojan Attacks

A Trojan as this program is suitably called, is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

There are many simple ways of installing a Trojan in someone's computer. To cite and example, two friends Rajan and Ramesh, had a heated argument over one girl, Radhika whom they both liked. When the girl, asked to choose, chose Ramesh over Rajan, Rajan determined to get even. On the 14th of February, he sent Mukesh a spoofed electronic card, which appeared to have come from Radhika's mail account. The electronic card actually contained a Trojan. As soon as Ramesh opened the card, the Trojan was fixed on his computer. Rajan now had complete control Ramesh's computer and proceeded to harass him thoroughly.

INTRODUCTION OF INFORMATION TECHNOLOGY ACT, 2000

In India, the Information Technology Act 2000 was agreed after the United Nation General Assembly Resolution A/RES/51/162, dated the 30th January, 1997 by adopting the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. This was the primary step towards the Law relating to electronic commerce at international level to regulate an another form of commerce and to give lawful status in the area of electronic commerce. It was enacted taking into consideration UNICITRAL model of Law on e- commerce 1996.

The IT Act, 2000

In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000.

This Act aims to provide the legal infrastructure for electronic commerce in India. And the cyber laws have a main effect for e-businesses and the modern economy in India. So, it is vital to understand what are the various perspectives of the IT Act, 2000 and what it offers.

The Information Technology Act, 2000 also aims to offer for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless or else agreed, an acceptance of contract may be expressed by electronic way of communication and the same shall have legal validity and enforceability. Some highlights of the Act are listed below:

Chapter-II of the Act specifically stipulates that any subscriber may check an electronic record by affixing his electronic signature. It further states that any person can verify an electronic record by use of a public key of the subscriber.

Chapter-III of the Act details about Electronic Governance and provides inter alia amongst others that where any law provides that information or any other matter shall be in writing or in the typewritten or written form, then, notwithstanding anything restricted in such law, such requirement shall be deemed to have been satisfied if such information or matter is -

rendered or made available in an electronic form; and accessible so as to be usable for a later reference. The said chapter also details the legal recognition of Digital Signatures.

Chapter-IV of the said Act gives a scheme for Regulation of Certifying establishments. The Act includes a Controller of Certifying Authorities who shall perform the function of exercising supervision over the actions of the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities as also mentioning the various forms and content of Electronic Signature Certificates. The Act recognizes the need for recognizing foreign Certifying Authorities and it further details the various requirements for the issue of license to issue Digital Signature Certificates.

Chapter-VII of the Act details about the scheme of things relating to Digital Signature Certificates. The duties of subscribers are also hallowed in the said Act.

Chapter-IX of the said Act talks about penalties and judgement for various offences. The penalties for loss to computer, computer systems etc. has been fixed as damages by way of reimbursement not more than Rs. 1,00,00,000 to affected persons. The Act talks of appointment of any officers not under the rank of a Director to the Government of India or an equivalent officer of state government as an Adjudicating Officer who shall decide whether any person has made a violation of any of the provisions of the said Act or rules designed there under. The said Adjudicating Officer has been given the powers of a Civil Court.

Chapter-X of the Act talks of the establishment of the Cyber Regulations Appellate Tribunal, which shall be an appellate body where appeals against the orders passed by the Adjudicating Officers, shall be preferred.

Chapter-XI of the Act talks about various offences and the said offences shall be checked only by a Police Officer not under the rank of the Deputy Superintendent of Police. These offences include altering with computer source documents, publishing of information, which is not decent in automatic form, and hacking.

The Act also provides for the constitution of the Cyber Regulations Advisory Committee, which shall advice the government as regards any rules, or for any other objective attached with the said act. The said Act also offers to change the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the IT Act.

CONCLUSION

The Information Technology Act 2000 was passed when the country was facing the problem of increasing cyber crimes. Since the Internet is the mediator for huge data and a large base of communications around the world, it is required to take specific precautions while functioning it. Therefore, in order to protect cyber crime it is vital to educate everyone and exercise safe computing.

REFERENCES

1. Cybercrime: A Tutorial from *Business Week*: February 21, 2000.
2. Charles L. Owens ,"Computer Crimes and Computer Related or Facilitated Crimes",Chief, Financial Crimes Section, Federal Bureau of Investigation, March 19, 1997
3. Paul Anderson ,FBI SAYSCYBERCRIME IS BECOMING AN "EPIDEMIC", ERRI Analyst
4. Marcel Dekker , "Security of the Internet", Published in The Froehlich/Kent Encyclopedia of Telecommunications vol. 15., New York, 1997, pp. 231-255.
5. John D. Howard , An Analysis Of Security Incidents On The Internet 1989 - 1995, A dissertation submitted to the graduate school in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Engineering and Public Policy , Pittsburgh, Pennsylvania 15213 USA, April 7, 1997