Prevention And Control Of Cyber Crimes

Dr. Navneet Kaur

Director (Computers)
Mohali, Punjab

Computers and their use is a day-to-day activity of all the students, professionals, teachers, universities, and banks, supermarkets, in the entertainment field, in medical profession and also in higher education. The use of this weapon is spreading vary widely in all parts of our society. As every weapon has two ways of operation, one is good and essential and the other is bad and not essential. Many times, whenever a new weapon is invented, many people use it unknowingly for the wrong purpose[i]. So to aware them and to make the proper use of the power of the newly invented weapon, laws are to be formulated and should be implemented.

Cyber crime is a generic term that refers to all criminal activities done using the medium of computers, the Internet, cyber space and the worldwide web. There isn't really a fixed definition for cyber crime. The Indian Law has not given any definition to the term „cyber crime". In fact, the Indian Penal Code does not use the term „cyber crime" at any point even after its amendment by the Information Technology (amendment) Act 2008, the Indian Cyber law But "Cyber Security" means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

The word "cyber law" encompasses all the cases, statutes and constitutional provisions that affect persons and institutions who control the entry to cyber space provide access to cyberspace, create the hardware and software which enable people to access cyberspace or use their own devices to go "online" and enter cyberspace. In simple way we can say that cyber crime is unlawful acts wherein the computer is either a tool or a target or both. Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given

birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

There has been confusion on the criteria used to determine the definition of the term Cyber Crimes or computer crimes. Some argued that, it is any crime that involves the use of computer; some argued that, it is a crime in the presence of a computer. However, some have criticized the categorization of cyber crime. Don Gotternbarn argued that there is nothing special on the crimes that happen to involve computers[ii]. Is it possible for a crime being categorized in accordance to a tool, equipment, mechanism or means through which it was committed? If that 'so, how many categories of crime would be there? How about the crime committed through using a television, automobiles, scalpel, scissors, and other tools, can we categorize each of them as individual crimes? Gotternbarn concludes that crimes involving computers are not necessarily issues in computer ethics

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[iii]:

1.Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

2.Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

Even though this definition is not completely definitive, however it gives us a good starting point, for determining just what cyber crime means, by incorporating computer crime and computer related crime.

Origin of Cyber Crime

Banks and other financial institutions were amongst the first large scale computer users in the private sector, for automate payroll and accounting functions. Therefore, fraud in a computer scheme emerged. One of the first cases cited as an instance of the computer fraud involved Equity-funding Corporation in the US, fraud was simple[iv].

The frauds succeed because the auditors and regulators accepted computer printouts as definitive evidence of policies and did no task original documentation[v]. When the fraud was discovered, some 64,000out of 97,000 policies allegedly issued by the company proved to be false, almost 1 Billion pounds estimated to be the loss.

Typology of Cyber Crime

In a traditional means, a term crime covers a broad range of offences. It is from this broad range, the typology or classification of cyber crime became difficult. A good example of an international instrument, which tried to categorize types of cyber crime, is the Council of Europe[vi] Convention on Cyber Crime, European Treaty Series -No. 185, Budapest, and 23.XI. 2001.

The Convention on Cyber Crime distinguishes between four different types of offences[vii]:

1.Offences against the confidentiality, integrity and availability of computer data and systems, such as illegal access, illegal interception, data interference, system interference, and misuse of devoice;

2.Computer-related offences, such as computer-related forgery and computer-related Fraud;

3.Content-related offences, such as offences related to child pornography;

4.Copyright-related offences, such as offences related to copyright infringements and related rights.

Cyber Extortion

Cyber extortion is a crime involving an attack or threat of attack coupled with a demand for money to avert or stop the attack[viii]. Cyber extortion can take many forms. Originally, denial of service (DoS) attacks against corporate websites were the most common method of cyber extortion; the attacker might initiate a ping storm and telephone the president of the company, demanding that money be wired to a bank account in a foreign country in exchange for stopping the attack.

In recent years, however, cybercriminals have developed ransom ware, which encrypts the victim's data. The extortionist's victim typically receives an email that offers the private decryption key in exchange for a monetary payment in Bitcoins, a digital currency. Cyber extortion can be lucrative, netting attackers millions of dollars annually. Unfortunately, as with other types of extortion, payment does not guarantee that further cyber-attacks will not be launched. Most cyber extortion efforts are initiated through malware in e-mail attachments or on compromised websites[ix]. To mitigate the risks associated with cyber extortion, experts recommend that end users should be educated about phishing exploits and back up there computing devices on a regular basis.

Conclusion

Cybercrime being global in character, generally affects the person far away from the place of offence, may it be in the same country or some other country. It, therefore, requires policing at international level as also the active cooperation of the international community. The European Convention on Cybercrime was indeed a praiseworthy attempt as it laid down guidelines to be followed by the member states in combating cybercrime.

A country wise assessment of cyber law indicates that only a few countries have updated their cyber law to counter the cyberspace crime effectively, while many of them have not even initiated steps to structure laws for policing against these crimes. This divergent approach of world nations towards the desirability of cyber law poses a real problem in management of the Internet crime and at the same time requires substantial scope for the cyber criminals to discharge detection and abuse. All the nations should therefore, realize the need and urgency for creating awareness about

the dangerous nature of cyber crimes, which are perpetuating illegal online activities in cyber space. Cyber misconduct is perhaps the extreme epidemic spread over the world in the new millennium, which has to be curtailed by adopting a global preventive strategy.

End note

[i] Christopher Reed, Internet Law; Text and Materials , 2000 at page 119

[ii] Herman T. Tavani, Ethics and Technology, Ethical Issues in an Age of Information and Communication Technology, 2nd Edition, John Wiley & Sons, Inc, 2007, United States of America, p.202.

[iii] Talwant Singh, District & Sessions Judge, Cyber Law & Information Technology, Delhi-India

[iv] Norman, Chapman and Hall Computer insecurity, 1983 at Pg. 199

[v] Cyber Crime… And punishment? Archaic Laws Threaten Global Information, a report prepared by McConnell International, 2000.

[vi] Gordon/Ford, On the Definition and Classification of Cyber Crime, Journal in Computer Virology, Vol.2, No. 1,2006, page 13-20.

[vii] Global Cyber Security Agenda/High-Level Experts Group, Global Strategic Report, 2008,at http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[viii] Cyberspace: United States Faces Challenges in Addressing Global Cyber security and Governance, Government Accountability Office, 2010

[ix] National Cyber security Strategy, The Netherlands, 2011