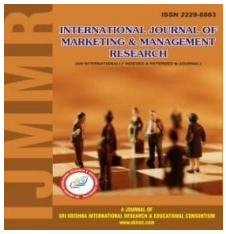
The Journal of Sri Krishna Research & Educational Consortium

INTERNATIONAL JOURNAL OF MARKETING AND MANAGEMENT RESEARCH

Internationally Indexed & Listed Referred e-Journal



E-CRIME: CHALLENGES FOR E-COMMERCE IN CHANGING ECONOMIC ENVIRONMENT IN INDIA

MISS. SANTOSHI A.PAWAR*

*Research Scholars.

ABSTRACT

"The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb". - National Research Council, "Computers at Risk", 1991.

Remarkable achievements in the IT sector is really a matter of pride to India but the associated problem that is causing serious concern is the rapid raise in cyber crimes. Internet has enabled the use of website communication, email and a lot of anytime anywhere IT solutions for the betterment of human kind. Internet, though offers great benefit to society, also present opportunities for crime using new and highly sophisticated technology tools. Today e-mail and websites have become the preferred means of communication. Organizations provide Internet access to their staff. By their very nature, they facilitate almost instant exchange and dissemination of data, images and variety of material. Regular stories featured in the media on computer crime include topics covering hacking to viruses, web-jackers, to internet pedophiles, sometimes accurately portraying events, sometimes misconceiving the role of technology in such activities. Both the increase in the incidence of criminal activity and the possible emergence of new varieties of criminal activity pose challenges for e-commerce, legal systems, as well as for law enforcement.

KEYWORDS: *E-Crime, E-Commerce, Cyber Crime, Cyber Law, I.T. Act, 2000, Internet Economy.*

INTRODUCTION

E-CRIME

• Computers are increasingly being targeted by criminals or used as tools to commit old and new types of crime.

• Legislative change to address the increase in and diversity of computer crime is in progress. However, policing computer crime is resource-intensive, complex and requires support from a number of organizations.

• There are several technologies available to improve computer security but their effectiveness may be limited without user awareness and education.

• Responsibility for securing computers against crime largely rests with the user (individual or organization), although there is debate over whether the government and industry should do more to protect users.

Cyber crime is an evil having its origin in the growing dependence on computers in modern life.

"A simple yet sturdy definition of cyber crime would be unlawful acts wherein the computer is either a tool or a target or both". 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 e-mail spoofing, cyber defamation, etc.

II. TYPES OF CYBER CRIME

Cyber Crime refers to all activities done with criminal intent in cyberspace. These fall into three slots.

- Those against persons.
- Against Business and Non-business organizations.
- Crime targeting the government.

III. E-COMMERCE

A. DEFINITION

Electronic commerce or e-commerce refers to a wide range of online business activities for products and services

E-commerce is the use of electronic communications and digital information processing technology in business transactions to create, transform, and redefine relationships for value creation between or among organizations, and between organizations and individuals.

Mobile phones, email and the Internet provide most scope for small businesses. Applications include Internet retailing, Internet banking and electronic settlements, browsing and customer selection of products and services. The Internet provides access 24 hours a day, seven days a week – any time – anywhere. Thus, time and place are no longer binding factors.

B. WHAT ARE THE DIFFERENT TYPES OF E-COMMERCE?

1. Business-To-Business (B2B);
2. Business-To-Consumer (B2C);

3. Business-To-Government (B2G);
4. Consumer-To-Consumer (C2C);
5. Mobile Commerce (M-Commerce).

• E-commerce is more about strategy and business management than it is about technology.

• Initiatives for a strategic approach to the digital economy require a dynamic and not static approach.

• It is essential to create a policy and regulatory environment that favors the development of e-commerce and harmonizes national approaches.

• For e-commerce promotion it is not just the hardware and physical infrastructure that is enough. What is required is the right 'info-structure' meaning.

• The issue is not whether the Internet should be regulated, but how.

• Certifying and authentication authorities that have to come up as a sequel to the IT Act need to be fully operational early.

• E-commerce in India encompasses three areas:

(i) Software exports

(ii) Web-enabled services

(iii) e-business and e-trade.

While it is generally agreed that the private sector should take the lead role in the development and use of e-commerce, the government plays an instrumental role in encouraging e-commerce growth through concrete practicable measures such as:

1. Creating a favorable policy environment for e-commerce; and

2. Becoming a leading-edge user of e-commerce and its applications in its operations, and a provider to citizens of e-government services, to encourage its mass use.

IV. INFORMATION TECHNOLOGY ACT, 2000

BACKGROUND OF INFORMATION TECHNOLOGY ACT, 2000 (CYBER LAW)

♦ United Nations Commission on International Trade Law (UNCITRAL) adopted a model law on Electronic Commerce in 1996.

♦ The United Nations in 1997 recommended that all member countries should give favorable consideration to that model law.

♦ In India the Information Technology Act (IT Act 2000) was passed in 2000, based on the model law. Date of commencement of the I.T. Act- 17.10.2000. It is a landmark Act in the direction of boosting E-commerce in India.

V. INITIATIVES TO PREVENT E-CRIME

A. INFRASTRUCTURE FACILITIES

The Directorate of Forensic Science under the Ministry of Home Affairs, with its three Computer Forensic Labs (CFLs) and three offices of Government Examiner of Questioned Documents (GEQDs) provides the necessary forensic analysis expertise to the Law enforcement agencies. Most of the States also have Forensic Science Laboratories, and some of the cyber crime cells at the state police stations also have limited facilities and expertise to handle common cyber crimes related to emails, pornography, hacking etc. However, the Central and State Forensic Laboratories are more conversant with conventional areas of forensics like Ballistics, Toxicology/Serology, Physical & Chemical sciences etc. and Computer/Cyber forensics has not yet been identified as an independent discipline in forensics. Cyber forensics is one amongst many other crime investigation facilities operated by these organizations and being a new area, have scanty infrastructure & trained personnel. Very few of them have facilities and expertise to meet the changing needs in cyber crime investigations.

Two technical resource centers, one focusing on computer disk forensics and the other on steganograhy, set up at Center for Development of Advanced Computing (CDAC) Thiruvananthapuram and Kolkata respectively, have been sponsored by DIT. These centers besides research also facilitate law enforcement agencies in cyber crime investigations.

b. TRAINING

For successful prosecution of cyber crimes it is essential to have adequate and cogent digital evidence against the suspect and then link this information to the suspect in a legally acceptable manner. Information stored in digital form is transient in nature and therefore law enforcement personnel require specialized skills to seize, collect, analyze and report digital evidence in a Court of Law.

Many organizations like NCRB-Delhi, CBI Academy- Ghaziabad, National Police Academy -Hyderabad etc conduct training programs, generally on computers software packages and fundamentals of cyber forensics. Some collaborative training programs with FBI are also conducted. CERT-IN, CCA, CFSL etc conduct some subject specific courses on Cyber Security, Cyber Laws, Cyber Crimes & related issues. In general, the courses on cyber forensic tools, their suitability for specific applications, comparisons, technology & crime trends, international best practices etc are rare or very few.

Police personnel are also frequently transferred to hold different assignments & hence there is a continuous need for training in the enforcement department. Also, as most of the crimes involve use of computers & electronic gadgets at some stage of committing the crime or the other, basic knowledge & training in digital evidence is always desirable and advantageous for the law enforcement personnel. There is an urgent need for conducting more training programs and there is scope for public private partnership as well as international cooperation in this area.

C. INTERNATIONAL COOPERATION

Cyber Crime cases are covered under Mutual Legal Assistance Treaties (MLATs), which India has with various countries. Moreover, India is a member of Cyber Crime Technology

Information Network System (CTINS), which is a Japanese Govt. initiative for mutual exchange of information regarding cyber crimes among the member countries, which is advisory in nature. This system is presently installed in the Cyber Crime Investigation Cell of Central Bureau of investigations (CBI), which is also 24x7 point of contact for Sub Group of Hi-tech Crimes of G-8 Countries.

D. INDUSTRY INITIATIVES

The two industry associations in India which are participating in major promotional activities in the IT sector are, National Association of Software and Service Companies (NASSCOM) and Manufacturer Association of Information Technology (MAIT). MAIT, initially set up for purposes of scientific, educational and IT industry promotion, has emerged as an effective and dynamic organization with majority of the Members coming from the Hardware Sector, by turnover, and the remaining from Training, Design, R&D and the associated services sectors of the Indian IT Industry. MAIT's charter is to develop a globally competitive Indian IT Industry, promote the usage of IT in India, strengthen the role of IT in national economic development and promote business through international alliances. The organization's special focus is on domestic market development and attracting foreign investment in the Indian IT Industry.

NASSCOM, the premier trade body and the chamber of commerce of the IT software and services industry in India was set up to facilitate business and trade in software and services and to encourage advancement of research in software technology. It is a not-for-profit organization. With over 1050 members, of which over 150 are global companies from the US, UK, EU, JAPAN AND CHINA, NASSCOM is a true global trade body, with member companies in the business of software development, software services, software products and it-enabled/BPO services.

Information Security remains one of the key priorities for the Indian IT Enabled Services –Business Process Outsourcing (ITES-BPO) industry, a challenge that has to be overcome in order to firmly establish the sector's credentials as a trusted sourcing destination. Recognizing the fact that security breaches in leading BPO firms can put a spanner in India's successful outsourcing run, the industry has come forward to devise roadmaps and outline strategies that will help create an impregnable Information Security environment. The country, in fact has been working very closely with representatives of the US market, the largest outsourcer of processes to India.

VI. CASE STUDY

1. CREDIT CARD FRAUD

Credit cards are commonly being used for online booking of airline and railway tickets and for other ecommerce transactions. Although most of e-commerce websites have implemented strong security measures (such as SSL, secure web servers etc), instances of credit card frauds are increasing.

The scenario: The victim's credit card information is stolen and misused for making online purchases (e.g. airline tickets, software, subscription to pornographic websites etc).

The law: Sections 43 and 66 of Information Technology Act and section 420 of Indian Penal Code.

Who is liable?

All persons who have stolen the credit card information as well as those who have misused it.

The motive: Illegal financial gain.

2. ONLINE SHARE TRADING FRAUD

With the advent of dematerialization of shares in India, it has become mandatory for investors to have Demat accounts. In most cases an online banking account is linked with the share trading account. This has led to a high number of online share trading frauds.

The scenario:

Scenario 1: The victim's account passwords are stolen and his accounts are misused for making fraudulent bank transfers.

Scenario 2: The victim's account passwords are stolen and his share trading accounts are misused for making unauthorized transactions that result in the victim making losses.

The law:

Scenario 1: Sections 43 and 66 of Information Technology Act and section 420 of Indian Penal Code.

Scenario 2: Sections 43 and 66 of Information Technology Act and section 426 of Indian Penal Code.

Who is liable?

Scenario 1: All persons who have stolen the account information as well as those who have misused it.

Scenario 2: All persons who have stolen the account information as well as those who have misused it.

The motive:

Scenario 1: Illegal financial gain

Scenario 2: Revenge, jealousy, hatred

3. USE OF INTERNET AND COMPUTERS BY TERRORISTS

Many terrorists are using virtual as well as physical storage media for hiding information and records of their illicit business. They also use emails and chat rooms to communicate with their counterparts around the globe.

The scenario: The suspects carry laptops wherein information relating to their activities is stored in encrypted and password protected form. They also create email accounts using fictitious details. In many cases, one email account is shared by many people.

The law: Terrorists are covered by conventional laws such as Indian Penal Code and special legislation relating to terrorism.

Who is liable?

Terrorists as well as those who help them to protect their information are liable. If email service providers do not assist the law enforcement personnel in the investigation then they are also legally liable.

The motive: Keeping terrorism related information confidential. Secure communication amongst terrorist group members.

4. VIRUS ATTACKS

Computer viruses are malicious programs that destroy electronic information. As the world is increasingly becoming networked, the threat and damage caused by viruses is growing by leaps and bounds.

The scenario:

Scenario 1: The virus is a general "in the wild" virus. This means that it is spreading all over the world and is not targeted at any specific organization.

Scenario 2: The virus targets a particular organization. This type of a virus is not known to anti-virus companies as it is a new virus created specifically to target a particular organization.

The law:

Scenario 1: Sections 43 and 66 of Information Technology Act and section 426 of Indian Penal Code.

Scenario 2: Sections 43 and 66 of Information Technology Act and section 426 of Indian Penal Code.

Who is liable?

Scenario 1: The creator of the virus.

Scenario 2: The creator of the virus as well as the buyer who purchases the virus (usually to target his business rivals).

The motive:

Scenario 1: Thrill and a perverse pleasure in destroying data belonging to strangers.

Scenario 2: Illegal financial gain, revenge, business rivalry.

5. WEB DEFACEMENT

Website defacement is usually the substitution of the original home page of a website with another page (usually pornographic or defamatory in nature) by a hacker.

Religious and government sites are regularly targeted by hackers in order to display political or religious beliefs. Disturbing images and offensive phrases might be displayed in the process, as well as a signature of sorts, to show who was responsible for the defacement.

Websites are not only defaced for political reasons, many defacers do it just for the thrill.

The scenario:

The homepage of a website is replaced with a pornographic or defamatory page. In case of Government websites, this is most commonly done on symbolic days (e.g. Independence Day of the country).

The law:

Sections 43 and 66 of Information Technology Act [In some cases section 67 and 70 may also apply].

Who is liable?

The person who defaces the website.

The motive: Thrill or a perverse pleasure in inciting communal disharmony.

VII. CONCLUSION

To combat cyber crime, India, besides ensuring a robust Information Security environment, has put up a legal framework in place, initiated awareness and training programs and set up cyber forensic facilities. However the cyber crime data for year 2005 indicates an increase in the crime rate, particularly in mega cities and more offenders are in the age group, 18-30 years which draws special attention and needs further studies to understand the motives, implications etc.

A developing country can become industrialized and modernized if it can extensively apply IT to enhance productivity and international competitiveness, develop e-commerce and e-governance applications.

An information-based society or knowledge based society is composed of IT products, IT applications in society and economy as a whole. Many countries in Asia are taking advantage of e-commerce through opening of economies, which is essential for promoting competition and diffusion of Internet technologies.The Internet is boosting efficiency and enhancing market integration in developing countries.

Indian IT act Amendment though has made a major attempt to address issues related to cyber crime; it still falls short on many counts. Some of the major shortcomings which we feel needs to be addressed are: Pornography, Data Protection, Spamming, and Identity Theft etc.

As country develops into a more robust economy and use of computers becomes ubiquitous, it is imperative that our laws are updated to respond to changing scenario. Quite unlike other penal laws IT Act in particular needs revision and reviews much more regularly mainly due to rapid changes in use of Information Technology.

VIII. REFERENCES

- "Cyber Crime & Corporate Liability" – first published by Wolters Kluwer in 2008.
- "Cyber Crime – Prosecution & Defense" – first published by Asian School of Cyber Laws in 2003 with revised editions published in 2005, 2006, 2007 and 2008).
- Cyber law : The Law of Internet by J. Rosenoer
- Cyber Law : The Indian Perspective By Pawan Duggal.
- Cyber Law & Its implication By J. Sruis
- "E-commerce in India: How to make it happen?" Report of the CII National Committee on E-Commerce 2000-2001 (Confederation of Indian Industry).
- Department of Telecommunication, India, Annual Report 2000-2001.
- e-commerce (India), October 2001. "Redefining business parameters".
- e-commerce (India), February 2002. "An e-fulfilment model and its application in the Indian context".
- e-commerce (India), April 2002. "Dot-coms are the future".
- e-commerce (India), April 2002. "The role of e-commerce in the new economy".
- Goldman Sachs, 2000. Report on IT Global Services (September 2000).
- Indian Express (Bombay), 7 June 2001. Statement of the Minister of Communication.
- NASSCON and BCG, 2001. E-Commerce Opportunities for India Inc. (by NASSCOM and The Boston Consulting Group) (July 2001).
- Electronic Commerce: Some Implications for Firms and Workers in Developing Countries, International Institute for Labour Studies, Geneva.
- Cyber Crime Today & Tomorrow, Thiru Dayanithi Maran, www.d.maran.nic.in/ speechdisplay.php.
- Police make headway, The Hindu, Sunday October 29, 2006.
- Cyber Crimes on the rise in state - Kerala: The Hindu Monday Oct 30 2006.
- Losses due to cyber crime can be as high as $40 billion, The Hindu Business line dt May 21 2007 downloaded 20 Oct2007.
- Phishing attacks against Indians: F-Secure, The Business line Monday July 23, 2007