International Journal of Law
ISSN: 2455-2194
www.lawresearchjournal.com
Volume 2; Issue 1; Jan 2016; Page No. 45-48

E-commerce, Cyber Crime and Indian cyber Law

Dr. Minakshi Kumawat
Independent Researcher, IRIS C-302, Magarpatta City, Hadapsar, Pune, Maharashtra, India.

Abstract
Gone by those days when people needed to plan a lot before going to buy things. Today the shopping is few clicks away on your computer or smart phone. E- Commerce is the key role player in bringing the whole world of choice of goods and services to your palm. Be it is shopping of goods or services, online shopping is the solution. *E-commerce* or E shopping involves transection of money while buying and selling the goods or transferring funds using computers. The goal of *E-commerce* technology is to give a secure, convenient and immediate payment facility to the users over the internet. But the internet world is full of threats, for the users to have a feeling of anonymity. Cybercrime threat is becoming a most damaging act to E- commerce in today's world which needs to be controlled by strong cyber laws. Indian Law has existing provisions to counteract cybercrime in India. Further stronger provisions will enable the society to bring the crimes under control.

Key Words: E-Commerce, Cyber Crime, Cyber Law, threats, secure payments. Civil Liability, Information Technology Act (ITA-2000), Information Technology Amended Act (ITAA-2008), Business to Customer (B2C), Business to Business (B2B), Customer To Customer (C2C)

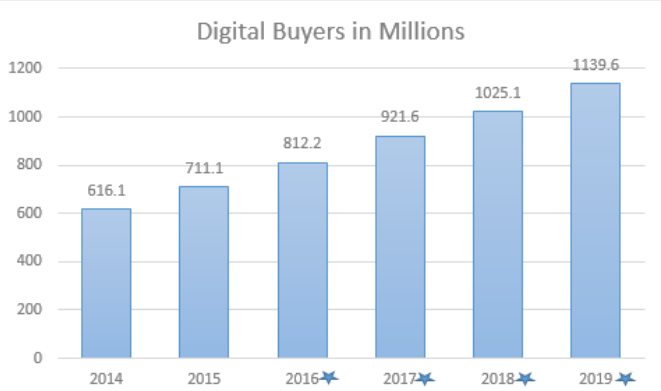
E-Commerce

Internet was born in 1953 but it was not so popular at that time. It was predominantly used for military communication purpose. It took 32 years when internet had a real birth and it went public in 1989. Since then, the internet had governed every aspect of our life starting from education, socializing with friends, Gaming or shopping. The involvement of internet in our life has increased exponentially in recent years. Today buying and selling is widely done over internet. E-commerce can be defined as any sort of transection made over internet. Buying over internet includes direct buying or buying through affiliates or agents. Selling over internet includes selling on your website, Selling on auction sites or selling on social networking sites. The growth of *E- commerce* in terms of business technology has created a ground for buying –selling of goods & services and it is driving key business processes inside the organisation. *E- Commerce* has its unique advantages where it gives tremendous amount of possibilities to all kind of business owners to grow their business exponentially. It provides reach to new markets over the web which will otherwise be impossible with their physical sales force. It brings commercial advantages to the businesses freeing them from huge investment on business space, traveling and investing time.

Internet connects the businesses to the individual customers or group of customers where private customers can order various products which they then receive by courier or postal mail. This model of E- commerce is called B2C. These businesses and customers are based in different parts of the world. The internet is the connecting links between the source supply and demand. Purchase of books from amazon, buying CDs DVDs from online stores and even online grocery shopping from Superstore is an example of Business to Customer E Commerce. There is another E- Commerce model where retailers connects to the whole sellers for their orders. This is called Business To Business (B2B) model. There is a third type of model where individual customer connects with customers, this is called Customer To Customer (C2C)

The *E-Commerce* sector has seen unpredicted growth in 2014. This growth was driven by rapid technological advancements where use of sophisticated devices such as smart phones and tablets and access to high speed wireless network created large online customer base.

As per Statista, (the statistical portal), 33 percent of the global market in 2015 and expected over 37 percent in 2018, the Asia Pacific Region (APAC) will become the leader of E-Commerce Industry. China is already set to outdo the United States as the single country with the largest E-commerce market in the world. India is another emerging e commerce market in APAC. As per the latest statistics, the retail E-Commerce Sales in India has exponentially grown from 2.3 billion USD in 2012 to 17.5 billion USD in 2015, showing an almost eight fold growth.



Source:- Statista 2016

The above data shows that the digital buyers will become almost double in 5 years from approx. 616 Millions in 2014 to approx. 1140 million in 2019.

Cyber Crime and its impacts on E-commerce

Introduction:-

On one side where E-commerce is becoming integral part and imparting convenience into lives, it is suffering from cybercrime. E-Commerce involves transection of Money and Information. Both of these things are of great importance for

the businesses. It is said that theft of information is more damaging then the theft of money. Cybercrime is rapidly growing under covered business operated by criminals, who trade valuable stolen financial information from millions of innocent internet users every year, in online black market. Cyber criminals do cyber-attacks on the computer systems through malware or malicious software, these takes control of the computer and gets access to the sensitive information stored in it, without users knowing about it. In more simple words, cyber-crime is the use of computer resources to involve in unofficial or illegal acts. For example, telemarketing and Internet fraud, identity theft and credit card account thefts are considered to be cybercrimes when the unlawful activities are committed through the use of a computer and the internet. It brings serious threats to the integrity and existence of the businesses and thus makes the need of strong security methods and laws, a top most priority.

Computer crimes covers a wide range of possible illegal activities. The crime can be generally be divided into two types of activities.

a. Direct targeting of the computer network or devices.
This includes

- Malware and malicious code.
- Denial of service attacks.
- viruses

b. Crime facilitated by computer networks or devices.
This includes

- Identity theft.
- Information warfare.
- Cyber stalking.
- Phishing scams.

Types of Cybercrimes

There are numerous types of cybercrimes. Some popular type of crimes are as below:-

Hacking: - This is the most popular type of crime, which is related to unauthorised access to the computer system. The computer system in broken into so that the sensitive information can be accessed. This involves use of variety of criminal software by hackers to gain access of a person's computer without him realising. This is different from ethical hacking.

Data theft:- This simply means stealing data, for normal or illegal usage. This happens when a person violets copyrights and steals music, movies, games and software. This type of crime is costing the copyright industry a huge money. The legal system is working on making stronger laws that prevent people from unlawful downloading.

Identity theft:- This is different from data theft. This produces a greater threat to the people using computer for transection and banking services. This is used to steal money or buy things through accessing credit/ debit card, bank account or any other sensitive information, by criminals in individual's name. This results into major financial loses or even vanishing the credit history.

Cyber Stalking:- This involves use of computer system to harass the victim. It has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals, to harass another individual, group of individuals, or organization. The behaviour includes false accusations, monitoring, the transmission of threats, identity theft, damage to data or equipment, the solicitation of minors for sexual purposes, and gathering information for harassment purposes.

Malicious Software:- Network disruption is the main aim of such software. These software are used to gain access to system and steal sensitive information or Data resulting damage to the software present in the system.

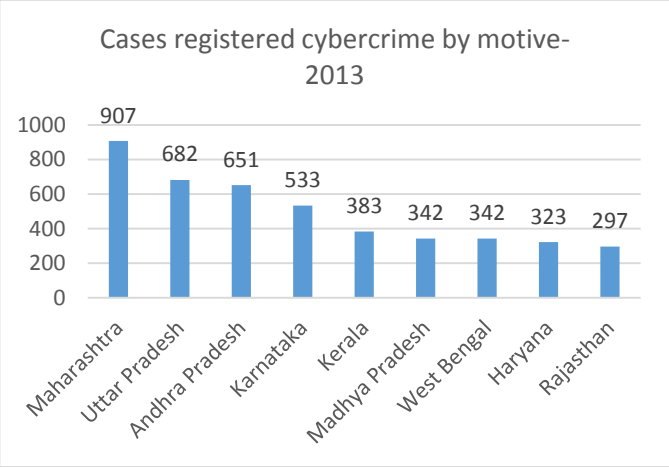
E-mail Bombing:- This is a form of net abuse comprising of sending large number of e-mails to an address. This is an attempt to flood the mail box or block the server where the account is hosted. These kind of e-mail bombs are simple to design and simple to detect and prevent.

Data Bidding:- Data bidding relates performing unauthorised modifications to data stored in the computer system. This includes unlawful changing the documents used for data entry.

Web Jacking:- Web Jacking is gaining access and taking control of others website, by hacker. The hackers can disfigure or even change the information on the site after web jacking. Normally this kind of crime is seen in fulfilling political objective or for demanding huge money from government organisations.

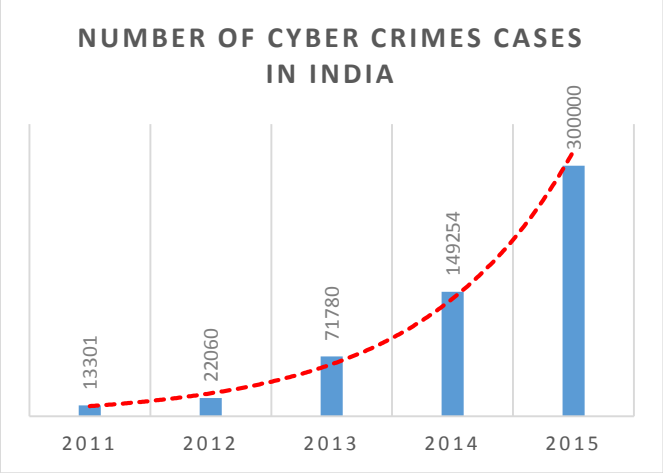
Child abuse:- In this type of crime, the criminals solicit minors through chat rooms for the purpose of child pornography. Security agencies spend large budget and time monitoring chat rooms, to reduce and prevent child abuse and soliciting.

From the above literature it is evident that the cybercrime is the biggest threat to the E-commerce. If we look at the statistics of damages, it is awful. No business can afford to ignore the cybercrime, which is estimated to cost global economy around 445bn USD a year. In India cybercrime is growing very rapidly. Below graph gives number of cases registered on cybercrime by motive in 2013, in top 9 states.



Source:- data.gov.in

Above statistics demonstrates the seriousness of cyber Crimes in India. The country has recorded 107% CAGR (Common Annual Growth Rate) in the number of Cyber Crimes registered in last few years. Maharashtra



Source: - ASSOCHAM- Mahindra SSG Report, Jan2015

From the above graph it is clear that the crime rate has increased exponentially (~22 times) in last 5 years. There were 13301 cases registered in 2011 which went almost double in following year. Increase between 2012 and 2013 was more than 200% (225%) in last two years the crimes has increased 100% to the previous year.

Cyber Law in India

Cyber law is a term used to describe the legal issues related to the unlawful activities on cyberspace, i.e. the internet. In nutshell cyber law is an attempt to counter the challenges presented by human activity in the cyberspace with legal system of laws applicable to the physical world.

In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government. The following Act, Rules and Regulations are covered under cyber laws:

1. Information Technology Act, 2000
2. Information Technology (Certifying Authorities) Rules, 2000
3. Information Technology (Security Procedure) Rules, 2004
4. Information Technology (Certifying Authority) Regulations, 2001

As stated in the preface of the IT Act, the objective of the IT Act-2000 is "to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

The Act essentially deals with the following issues:

a. Legal Recognition of Electronic Documents
b. Legal Recognition of Digital Signatures
c. Offenses and Contraventions
d. Justice Dispensation Systems for cybercrimes

In 2008 an amendment was brought in the IT Act2000 to make it more Information Technology focused, and to include the provisions required against latest cybercrimes. The Information Technology Amended Act 2008 was made effective from 27 Oct 2009.

Some of the notable features of the ITAA are as follows:

1. Focussing on data privacy
2. Focussing on Information Security
3. Defining cyber café Making digital signature technology neutral
4. Defining reasonable security practices to be followed by corporate
5. Redefining the role of intermediaries
6. Recognising the role of Indian Computer Emergency Response Team
7. Inclusion of some additional cybercrimes like child pornography and cyber terrorism.
8. Authorizing an Inspector to investigate cyber offences (as against the DSP earlier)

Chapter IX of ITAA deals with the penalties, compensation and Adjudication which is a major step towards fighting data theft, claiming compensation, introduction of security practices. This is detailed in section 43 of the ITAA act. This section addresses the civil offence of theft of data. If someone without permission of owner or any other person who is in charge of a computer, accesses or downloads, copies or extracts any data or introduces any computer contaminant like virus or damages or disrupts any computer or denies access to a computer to an authorised user or tampers etc…he shall be liable to pay damages to the person so affected. Earlier in the ITA -2000 the maximum damages under this head was Rs.1 crore, which (the ceiling) was since removed in the ITAA 2008. At heart, Section 43 is related to **Civil Liability.** Data Theft related criminal issues are dealt separately in section 65 and 66. This section covers offences related to writing a virus program or spreading a virus mail, a bot, a Trojan or any other malware in a computer network or causing a Denial of Service Attack in a server, and provision compensation through civil liability.

ITA-2000 has triggered amendments to existing acts to include IT offences related provisions. Below is the list of other main Acts which are amended by ITA.

1. **The Indian Penal Code, 1860:-** ITA 2000 has amended the section dealing with records and documents in the IPC by inserting word 'Electronic' there by treating the electronic records and documents on a par with physical records and documents.
2. **The Indian Evidence Act 1872:-** Prior to passing the ITA, all evidences in a court were in the physical form only. With the ITA giving recognition to all electronic records and documents. In the definitions part of the Act itself, the "all documents including electronic records" were substituted. Words like 'digital signature', 'electronic form', 'secure electronic record' 'information' as used in the ITA, were all inserted to make them part of the evidentiary mechanism in legislations.

Conclusion

To conclude, it will not be inappropriate to say that today's world is riding fast on the silicon chip horse which is controlled by the fibre optic Bridles. E-commerce has internet at its heart and spreading fast to every corner of the world. E-commerce has connected people to shrink the distances from thousands of miles to nanoseconds. This has become back bone of world economy. Cybercrime is like termite to this back-bone which is continuously threatening the economy. Though there are tough provisions in Indian IT act but the question is to implement these provisions and recommendations to bring the criminals to the justice. The criminals are so sharp to catch them. Day by day the research and technology in cybercrime world is becoming more and more advance. Along with E-commerce crimes, now the world will encounter cyber terrorism. As per a report by United States Institute of Piece, Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."

The need is to develop techniques to first protect the system and then catch the cyber criminals. There is a continuous need of research to develop technologies which is cybercrime immune. This will be the ideal E-world.

References

1. http://www.statista.com/topics/2454/e-commerce-in-india/
2. N Leena, Cyber Crime Effecting E-commerce Technology, Oriental Journal of Computer Science & Technology- Vol. 4(1), 209-212 (2011),
3. The 2013 eCommerce Cyber Crime Report: Safeguarding Brand And Revenue This Holiday Season, RSA Security-Oct2013
4. http://www.crossdomainsolutions.com/cyber-crime/
5. http://dazeinfo.com/2015/01/06/cyber-crimes-in-india-growth-2011-2015-study/
6. http://www.iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf.