International Journal of Research in Engineering, Science and Management
Volume-1, Issue-7, July 2018
www.ijresm.com ISSN (Online): 2581-5782

Cyber Extortion

Anmol Goyal[1], Priyanka Singh[2]

[1,2]Student, Department of Law, BVDU New Law College, Pune, India

***Abstract*: The research paper studies the concept of cyber extortion. The obstacles which comes in the way of using cyber technology and its criminal misuse. In today's Electronic world nothing is secure, everything can be hacked and misused. The main focus of the paper is on the laws prevalent in India and in other countries for this crime. The study is based on how the concept of cyber extortion comes to world.**

Key Words: cyber extortion

1. Introduction

CYBER EXTORTION is a crime involving an attack or threat of an attack coupled with a demand for money to avert or stop the attack". It is a hijacking activity that infects a computer with a malicious code that encrypts user based documents, then ransoms for a key than can be used to decipher them. Although many people have a limited knowledge of 'cyber extortion'. This kind of crime has a serious potential for serious impacts on our lives and society, because our society is becoming an information society, full of information exchange happening in cyber space. Thus it is necessary to introduce this topic 'cyber extortion' in detail i.e. focusing on the laws prevalent in India and in other countries for this crime. In this research paper we will first talk about the definition, origin of cybercrime, penalties that are engaged in India and in other world.

A. Research Methodology

This research is based on information and interpretations. Drafting and research is based on the secondary data provided by existing laws framed and amended in India as well as on the international front. Therefore research is doctrinal in nature.

B. Scope of Research

Through this dissertation we shall be primarily focusing upon the laws prevalent in India and in other countries and the penalties about this crime in India and in other countries.

C. Significance

This research is important because now-a-days individuals have used extortion as a means of making money for as long as crime has existed. However past schemes generally involved harm to expensive objects or even the victims themselves. While these kinds of scams are still very prevalent in today's world. Therefore to get more aware about this crime. This research is very much important.

D. Research Questions

1. Are the stringent penalties for cyber extortion in India?
2. What are the differences in laws in India and in other countries for this crime?

2. Origin of Cyber Crime

The first recorded cybercrime took place in the year 1820! That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage.

In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cybercrime.

Today computers have come a long way, with neural networks and Nano-computing promising to turn every atom in a glass of water into a computer capable of performing a Billion operations per second.

Cyber-crime is an evil having its origin in the growing dependence on computers in modern life. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants is being run on computers, cyber-crime has assumed rather sinister implications. Major Cyber-crimes in the recent past include the Citibank rip off. US $ 10 million were fraudulently transferred out of the bank and into a bank account in Switzerland. A Russian hacker group led by Vladimir Kevin, a renowned hacker, perpetrated the attack. The group compromised the bank's security systems. Vladimir was allegedly using his office computer at AO Saturn, a computer firm in St. Petersburg, Russia, to break into Citibank computers. He was finally arrested on Heathrow airport on his way to Switzerland

Types of cyber crime

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

Let us examine the acts wherein the computer is a tool for an unlawful act. This kind of activity usually involves a modification of a conventional crime by using computers. Some examples are:

A. Financial Crimes

This would include cheating, credit card frauds, money laundering etc. To cite a recent case, a website offered to sell Alphonso mangoes at a throwaway price. Distrusting 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 spread like wildfire. Thousands of people from all over the country responded and ordered mangoes by providing their credit card numbers. The owners of what was later proven to be a bogus website then fled taking the numerous credit card numbers and proceeded to spend huge amounts of money much to the chagrin of the card owners.

B. Sale of Illegal Articles

This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication.

C. Online Gambling

There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

D. Intellectual Property Crimes

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

E. Email Spoofing

A spoofed email is one that appears to originate from one source but actually has been sent from another source. E.g. beza has an e-mail address beza@bezaspeaks.com. His enemy, Dorexi spoofs his e-mail and sends obscene messages to all her acquaintances. Since the e-mails appear to have originated from Beza, his friends and business partners could take offence and relationships could be spoiled for life.

Email spoofing can also cause monetary damage. In an American case, a teenager made millions of dollars by spreading false information about certain companies whose shares he had short sold. This misinformation was spread by sending spoofed emails, purportedly from news agencies like Reuters, to share brokers and investors who were informed 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 thousands of investors lost a lot of money.

F. Forgery

Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners. These are made using computers, and high quality scanners and printers. In fact, this has becoming a booming business involving thousands of Pula being given to student gangs in exchange for these bogus but authentic looking certificates.

G. Cyber Defamation

This occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

H. Cyber Stalking

The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.

3. Indian Scenario

India is trying to implement the Digital India poor track record project to the best of its capabilities. The success of Digital India project would depend upon maximum connectivity with minimum cyber security risks. This is also a problem for India as India has a of cyber security.

According to Home Ministry statistics, as many as 71,780 cyber frauds were reported in 2013, while 22,060 such cases were reported in 2012. There have been 62,189 incidents of cyber frauds till June 2014.

In 2013, a total of 28,481 Indian websites were hacked by various hacker groups spread across the globe. The numbers of hacking incidents were 27,605 in 2012 and 21,699 in 2011.

As per the cyber-crime data maintained by National Cyber Records Bureau, a total of 1,791, 2,876 and 4,356 cases were registered under the Information Technology Act in 2011, 2012 and 2013, respectively. A total of 422, 601 and 1,337 cases were registered under cyber-crime related sections of the Indian Penal Code in 2011, 2012 and 2013, respectively.

There has been an annual increase of more than 40 per cent in cyber-crime cases registered in the country during the past two-three years,

According National Crime Records Bureau (NCRB), a total of 288, 420, 966, 1,791 and 2,876 cyber-crime cases were registered under IT Act during 2008, 2009, 2010, 2011 and 2012, respectively. As per the information reported to and tracked by Indian Computer Response Team (CERT-In), a total number of 308, 371 and 78 government websites were hacked during the years 2011, 2012 and 2013 respectively and 16,035 incidents related to spam, malware infection and system break-in were reported in 2013.

4. Global Scenario

International cybercrimes often challenge the effectiveness of domestic and international law and law enforcement. Because existing laws in many countries are not tailored to deal with cybercrime, criminals increasingly conduct crimes on the Internet in order to take advantages of the less severe punishments or difficulties of being traced. No matter in developing or developed countries, governments and industries has gradually realized the colossal threats of cybercrime on economic and political security and public interests. However, complexity in types and forms of cybercrime increases the difficulty to fight back. In this sense, fighting cybercrime calls for international cooperation. Various organizations and governments have already made joint efforts in establishing global standards of legislation and law enforcement both on a regional and on an international scale. U.S.-China's cooperation is one of the most striking progress recently because they are the top two source countries of cybercrime.

Information and communication technology (ICT) plays an important role in helping ensure interoperability and security based on global standards. General countermeasures have been adopted in cracking down cybercrime, such as legal measures in perfecting legislation and technical measures in tracking down crimes over the network, Internet content control, using public or private proxy and computer forensics, encryption and plausible deniability, etc. Due to the heterogeneity of law enforcement and technical countermeasures of different countries, this article will mainly focus on legislative and regulatory initiatives of international cooperation.

I. International Trends

As more and more criminals are aware of potentially large economic gains that can be achieved with cybercrime, they tend to switch from simple adventure and vandalism to more targeted attacks, especially platforms where valuable information highly concentrates, such as computer, mobile devices and the Cloud. There are several emerging international trends of cybercrime.

- *Platform switch:* Cybercrime is switching its battle ground from Windows-system PCs to other platforms, including mobile phones, tablet computers, and VoIP. Because a significant threshold in vulnerabilities has been reached. PC vendors are building better security into their products by providing faster updates, patches and user alert to potential flaws. Besides, global mobile devices' penetration—from smart phones to tablet PCs—accessing the Internet by 2013 will surpass 1 billion, creating more opportunities for cybercrime. The massively successful banking Trojan, Zeus is already being adapted for the mobile platform. Smishing, or SMS phishing, is another method cyber criminals are using to exploit mobile devices, which users download after falling prey to a social engineering ploy, is designed to defeat the SMS-based two-factor authentication most banks use to confirm online funds transfers by customers. VoIP systems are being used to support vishing (telephone-based phishing) schemes, which are now growing in popularity.
- *Social engineering scams:* It refers to a non-technical kind of intrusion, in the form of e-mails or social networking chats that relies heavily on human interaction and often involves fooling potential victims into downloading malware or leaking personal data. Social engineering is nevertheless highly effective for attacking well-protected computer systems with the exploitation of trust. Social networking becomes an increasingly important tool for cyber criminals to recruit money mules to assist their money laundering operations around the globe. Spammers are not only spoofing social networking messages to persuade targets to click on links in emails — they are taking advantage of users' trust of their social networking connections to attract new victims.
- *Highly targeted:* The newest twist in "hypertargeting" is malware that is meant to disrupt industrial systems — such as the Stuxnet network worm, which exploits zero-day vulnerabilities in Microsoft. The first known copy of the worm was discovered in a plant in Germany. A subsequent variant led to a widespread global outbreak.
- *Dissemination and use of malware:* malware generally takes the form of a virus, a worm, a Trojan horse, or spyware. In 2009, the majority of malware connects to host Web sites registered in the U.S.A. (51.4%), with China second (17.2%), and Spain third (15.7%). A primary means of malware dissemination is email. It is truly international in scope.
- *Intellectual property theft (IP theft):* It is estimated that 90% of the software, DVDs, and CDs sold in some countries are counterfeit, and that the total global trade in counterfeit goods is more than $600 billion a year. In the USA alone, IP theft costs businesses an estimated $250 billion annually, and 750,000 jobs.

J. International Responses

- *G8:* Group of Eight (G8) is made up of the heads of eight industrialized countries: the U.S., the United Kingdom, Russia, France, Italy, Japan, Germany, and Canada.

In 1997, G8 released a Ministers' Communiqué that includes an action plan and principles to combat cybercrime and protect data and systems from unauthorized impairment. G8 also mandates that all law enforcement personnel must be trained and equipped to address cybercrime, and designates all member countries to have a point of contact on a 24 hours a day/7 days a week basis.

- *United Nations:* In 1990 the UN General Assembly adopted a resolution dealing with computer crime legislation. In 2000 the UN GA adopted a resolution on combating the criminal misuse of information technology. In 2002 the UN GA adopted a second resolution on the criminal misuse of information technology.
- *ITU:* The International Telecommunication Union (ITU), as a specialized agency within the United Nations, plays a leading role in the standardization and development of telecommunications and cybersecurity issues. The ITU was the lead agency of the World Summit on the Information Society (WSIS).

In 2003, Geneva Declaration of Principles and the Geneva Plan of Action were released, which highlights the importance of measures in the fight against cybercrime. In 2005, the Tunis Commitment and the Tunis Agenda were adopted for the Information Society.

- *Council of Europe:* Council of Europe is an international organisation focusing on the development of human rights and democracy in its 47 European member states. In 2001, the Convention on Cybercrime, the first international convention aimed at Internet criminal behaviors, was co-drafted by the Council of Europe with the addition of USA, Canada, and Japan and signed by its 46 member states. But only 25 countries ratified later. [8] It aims at providing the basis of an effective legal framework for fighting cybercrime, through harmonization of cybercriminal offences qualification, provision for laws empowering law enforcement and enabling international cooperation.

5. Cyber Law in India Global Scenario Penalties in India and in Different Countries

A. Emergence of Information Technology Act, 2000

In India, the Information Technology Act 2000 was enacted 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 first step towards the Law relating to e-commerce at international level to regulate an alternative form of commerce and to give legal status in the area of e-commerce. It was enacted taking into consideration UNICITRAL model of Law on e- commerce 1996.

Some Noteworthy Provisions under the Information Technology Act, 2000.

- Sec.43 Damage to Computer system etc. - Compensation for Rupees 1crore.
- Sec.66 Hacking (with intent or knowledge) - Fine of 2 lakh rupees, and imprisonment for 3 years.
- Sec.67 Publication of obscene material in e-form - Fine of 1 lakh rupees, and imprisonment of 5 years, and double conviction on second offence.
- Sec.68 not complying with directions of controller - Fine up to 2 lakh and imprisonment of 3 years.
- Sec.70 attempting or securing access to computer - Imprisonment up to 10 years.
- Sec.72 for breaking confidentiality of the information of computer - Fine up to 1 lakh and imprisonment up to 2 years.
- Sec.73 Publishing false digital signatures, false in certain particulars - Fine of 1 lakh, or imprisonment of 2 years or both.
- Sec.74 Publication of Digital Signatures for fraudulent purpose - Imprisonment for the term of 2 years and fine of 1 lakh rupees.

B. International Cybercrime Conventions

- African Union Convention on Cyberspace Security and Personal Data Protection
- Council of Europe Convention on Cybercrime (also known as the Budapest Convention on Cybercrime).

Model Laws:

- CW Model Law – Model Law on Computer and Computer-related Crime
- SADC Model Law – SADC Model Law on Computer Crime and Cybercrime
- HIPCAR – Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbeans (Cybercrime/e-Crimes)
- ITU – International Telecommunications Union Cybercrime Legislation Resources – ITU Toolkit for Cybercrime Legislation

Some specific cybercrime law:

- Cybercrimes and Cybersecurity Bill (Cyber Bill) – South Africa (South Africa signed the Budapest Convention in 2001)
- Cyber security Information Sharing Act (CISA) – United States of America (this Bill has recently been passed by the US Senate)
- EU Network and Information Security Directive
- Criminal Code Act 1995 Australia
- Cybercrime Act 2001 Australia
- Chapter 08:06 (Cybercrime and Computer- related Crimes) Botswana
- Computer Misuse Act, 2007 Brunei Darussalam
- Criminal Code of Canada, Canada
- Cyber security Law China
- Criminal Code France
- Computer Crimes Act Malaysia
- Crimes Act,1961 New Zealand
- Cybercrime Prevention Act of 2012 – Philippines
- Act on Computer Crimes Thailand
- Cybercrimes Act, 2015 Tanzania
- UK – Computer Misuse Act, 2013
- United States Code USA

6. Conclusion

No one can deny the positive role of the cyber space in today’s world either it be political, economic, or social sphere of life. But everything has its pro’s and corns, cyber terrorists have taken over the technology to their advantage. To curb their activities, the Information Technology Act 2000 came into existence which is based on UNICITRAL model of Law on e-commerce. It has many advantages as it gave legal recognition to electronic records, transactions, authentication and certification of digital signatures, prevention of computer crimes etc. but at the same time is inflicted with various drawbacks also like it doesn’t refer to the protection of Intellectual Property rights, domain name, cyber-squatting etc. This inhibits the corporate bodies to invest in the Information technology infrastructure. Cases like Dawood and Quattrochi clearly reveals the problem of enforceability machinery in India. Cryptography is new phenomenon to secure sensitive information. There are very few companies in present date which have this technology. Other millions of them are still posed to the risk of cyber-crimes.

There is an urgent need for unification of internet laws to reduce the confusion in their application. For e.g. for publication of harmful contents or such sites, we have Indian Penal Code (IPC), Obscenity Law, Communication Decency law, self-regulation, Information Technology Act 2000 ,Data Protection Act, Indian Penal Code, Criminal Procedure Code etc but as they deal with the subject vaguely therefore lacks efficient enforceability mechanism. Due to numerous Laws dealing with the subject there lays confusion as to their applicability, and none of the Law deals with the subject specifically in toto. To end the confusion in applicability of Legislation picking from various laws to tackle the problem, i would suggest unification of laws by taking all the internet laws to arrive at Code which is efficient enough to deal with all the problems related to internet crimes. Although these legislations talk about the problem but they don't provide an end to it. There's need for a one Cyber legislation which is co-ordinated to look after cyber-crimes in all respects. With passage of time and betterment of technology in the present date, has also resulted in numerous number of Information technology related crimes therefore changes are suggested to combat the problem equally fast.

Crucial aspect of problem faced in combating crime is that, most of the countries lack enforcement agencies to combat crime relating to internet and bring some level of confidence in users. Present law lacks teeth to deter the terrorist groups for committing cyber-crimes if you see the punishment provides by the Act it's almost ineffective, inefficient and only provides punishment of 3 years at the maximum. Harsher laws are required at this alarming situation to deal with criminals posing threat to security of funds, information, destruction of computer systems etc. Data protection, by promotion of general principles of good information practice with an independent supervisory regime, would enable the law to maintain sufficient flexibility to achieve an appropriate balance between the need to protect the rights of the individuals and to have a control over the way their personal information have been used would be helpful in this increasingly networked economy. Just having two provisions in the Information Technology Act, 2000 for protection of data without any proper mechanism for to tackle the crime makes their mention in the Act redundant.

Information Technology Act is applicable to all the persons irrespective of their nationalities (i.e. to non-citizens also) who commits offence under the Information Technology Act outside India, provided the act or conduct constituting the offence or contravention involves computer, computer systems, or computer networks located in India under Section 1 and Section 75 of the Information Technology Act, but this provision lacks practical value until and unless the person can be extradited to India. Therefore it's advised that we should have Extradition treaties among countries. To make such provisions workable.

It's like 'eye for an eye' kind of situation where the technology can be curbed only by an understanding of the technology taken over by cyber terrorists. Even if the technology is made better enough to curb the computer related crime there is no guarantee if that would stay out of reach of cyber terrorists. Therefore Nations need to update the Law whether by amendments or by adopting sui generic system. Though Judiciary continues to comprehend the nature of computer related crimes there is a strong need to have better law enforcement mechanism to make the system workable.

References

[1] Indian Law Journal
[2] Researchgate.net (Online)
[3] Lexis Nexis
[4] International Journal of Scientific & Engineering Research
[5] www.cisecurity.org/cyber-extortion-an-industry-hot-topic/
[6] www.iup.edu