SJIF Impact Factor: 6.260| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)

EPRA International Journal of Research and Development (IJRD)

Volume: 5 | Issue: 1 | January 2020 - Peer Reviewed Journal

UNDERSTANDING CYBER CRIME AND CYBER LAUNDERING: THREAT AND SOLUTION

Dr.M.Suganya Aravazhi,

Post-Doctoral Fellow, Department of Sociology,University of Madras, Chennai.

Article DOI: https://doi.org/10.36713/epra3902

ABSTRACT

Cybercrime is an illegal action committed in the area of ITC and it is high speed, low cost and high tech offence. This kind of activity usually involves a modification of a conventional crime by using computers. The term 'cyber-laundering' is the practice of money laundering carried out in cyber space through online transactions. This article presents the meaning of cyber laundering dealing with offences concerned with the abuse of computers or other electronic gadgets. Cyber criminals also target at loopholes of mobile devices and the threats are growing faster than it does on personal computer. An effective legal frame work for combating cybercrime is important to develop the correct conceptual apparatus. Cyber criminals often favour those e-commerce portals and payment system where a great number of personal information and credit card data are being stored and processed. On the whole, an effective anti-cybercrime strategy is the need of the hour.

KEY WORDS: *Cybercrime, Money laundering, Information technology, Cyber security, Electronic gadgets, Financial services.*

INTRODUCTION

At present Information Technology and Communication (ITC) has become integral part of every aspect of human life. These have led to the integrated global information environment and every one can access any information in any place around the world without face to face contact. According to internet world states, there are 4.53 billion people (58.8%) are active internet users (June 2019) in the world. The internet user is capable of accessing information on the round the clock basis, can quickly share information with other users. The banking sector is one of the industries; heavily depend on modern technologies and internet. Cybercrime is an illegal action committed in the area of ITC and it is high speed, low cost and high tech offence.

According to UNO expert recommendations, the term of 'cybercrime' covers any crime committed by using computer system or networks, within their framework or against them. Theoretically, it embraces any crime that can be committed in the electronic environment. In other words, crimes committed by using e-computers against information processed and applied in the internet can be referred to cybercrimes.

Cybercrimes are punishable by the Information Technology Act, would be unsuitable as the Indian Penal Code also covers many cybercrimes, such as email spoofing and cyber defamation, sending threatening emails etc. A simple yet study definition of cybercrime would be 'Unlawful acts wherein the computer is either a tool or a target or both'. The computer is a tool for an unlawful act. This kind of activity usually involves a modification of a conventional crime by using computers. This article presents the meaning of cyber laundering dealing with offences concerned with the abuse of computers or other electronic gadgets. Crime in any form adversely affects all the members of the society. In developing countries, cybercrime has increased at rapid strides (DOJ, 2017). The term 'cyber-laundering' is the practice of money laundering carried out in cyber space through online transactions. Unlike the conventional money laundering the online transactions offer a wide range, speed and low cost for money laundering perpetrators can launch their actions as long as there is internet access.

REVIEW OF LITERATURE

Cassim (2009), explained In his article 'Formulating specialized legislation to address the growing spectre of cybercrime: A comparative study'. The cyber legislation formulated to address cybercrime in the United States of America, The United Kingdom, Australia, India, The gulf Countries and South Africa. The study reveals that the inability of national laws to address the challenges posed by cybercrime has led to the introduction of specialized cyber legislation. It is advocated that countries should introduce new cyber laws to respond to the rapid change in technology and cybercrimes. There should be continuous research and training of IT security personnel, financial service sector personnel, police officers, prosecutors and the judiciary to keep them abreast of the evolving technology.

Ultrascan (2014), stated that the loss of money is not the only risk that advance fee fraud imposes. In some cases, victims are lured to the home countries of the fraudster as part of the scheme, such as Nigeria where these scams are highly prevalent. If successful, the victim is kidnapped and held for ransom for more money. Nigeria tends to be the well-known as a top source of advance fee fraud schemes, but others include South Africa, Ghana, and the United States.

CYBER CRIME

At present the banking systems of most countries provide broad enough opportunities for online financial resources. 'Customer – Internet – Bank' and 'Telephone Banking' are the most widespread online banking services. Vulnerabilities of the financial system to cybercrime are to a large extent associated with insufficient protection of banking information. Cyber criminals also target at loopholes of mobile devices and the threats are growing faster than it does on personal computer (Animesh etal, 2017). The Budapest convention being the fundamental instrument provides the following categorization of cybercrime. a) Offences against the confidentiality, integrity and availability of computer data and systems, b) Computer related offences, including forgery and fraud committed with the use of computers, c) Content related offences, including child pornography, racism and xenophobia and d) Offences related to infringements of copy right and related rights.

An effective legal frame work for combating cybercrime is important to develop the correct conceptual apparatus. It is necessary to strengthen the responsibility of service providers to monitor the use of their services and as a means of encouraging them to reduce the risk of illegal use of their services.

The new technologies adopted by financial institutions are making them increasingly vulnerable to various risks such as phishing, identity theft, card skimming, vising, SMS sending, viruses and Trojans, spyware and adware, social engineering website cloning and cyber stalking (Syed etal, 2015).

Currently, 74% of the Indian population has mobile phone apps. According to RBI records, 22 million of the 589 million bank account holders use mobile banking apps. The volume of mobile banking transactions are 1,018,510 million INR in 2016 and as per the Global Financial Integrity Report, the total amount of illicit money moving out of India rose to 439.59 billion USD (28 lakh crore INR) from 2003 to 2012. In 2012, India ranked third globally with an estimated 94.76 billion USD (nearly 6 lakh crore INR) in illicit wealth outflows. Based on 2013 Norton report, India ranks among the top 5 countries in terms of number of cybercrime incidents such as ransom ware,and identity theft.

Around 65% of the total fraud cases reported by banks were technology related frauds, whereas advance related fraud accounted for a major proportion of the total amount involved in fraud. KYC (Know Your Customer) details are collected and assessed by the institutions at the time of customer on boarding as well as during re-KYC. A fraudster can find an opportunity to use incorrect KYC details during the customer life cycle to commit fraud. This process enables the criminal to enjoy profits without jeopardizing their source. Online financial services offer the option of enacting multiple, worldwide financial transactions very quickly, wire transfers

replaced the transport of hard cash. In general cybercrime has three categories:
1) Target cybercrime: The crime in which a computer is the target of the offense,
2) Tool cybercrime: The crime in which a computer is used as a tool in committing the offense and
3) Computer incidental: The crime in which a computer plays a minor role in committing the offense.

Cyberspace is an intangible dimension that is impossible to govern and regulate using conventional law. Cyber space handles gigantic traffic volumes every second. The primary source of cyber law in India is the Information Technology Act 2000. The reasons for the vulnerability of computers are: a) Capacity to store data in comparatively small space, b) Easy to access, c) Complex and d) Loss of evidence. Since, Internet was invented, people began to exchange information based on network of computers also keep data in computer rather than paper. Cyber law encompasses laws relating to 1) Cybercrimes, 2) Electronic and digital signatures 3) Intellectual property and 4) Data protection and privacy (Juneed and Bilal, 2017).

FORMS OF CYBER CRIME

Email spoofing is a forgery of an email header. This means that the message appears to have received from someone or somewhere other than the genuine or actual source. These tactics are usually used in spam campaigns or in phishing, because people are probably going to open an electronic mail or an email when they think that the email has been sent by a legitimate source. **Hacking** refers to the secretively breaking into the computer system and stealing valuable data from the system without any permission. **Spreading computer virus** is a set of Cyber instructions which are able to perform some malicious operations. Viruses stop the normal functioning of the system programs and insert few abnormalities. A computer viruses can be spread through- Emails, CDs, pen drives (secondary storage), Multimedia, Internet.

Phishing refers to stealing information's like passwords, credit card details, user names of target person over the internet. It is carried out by email spoofing and instant messaging. In this type of crime hackers make a direct link which directs the targeted persons to the fake page which looks and feels identical to the actual one. **Cyber stalking** is use of the Internet or other electronic means to stalk someone. This term is used interchangeably with online harassment and online abuse. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property (Leukfeldt etal, 2016).

Cyber defamation means the harm that is brought on the reputation of an individual in the eyes of other individual through the cyber space. The purpose of making defamatory statement is to bring down the reputation of the individual. **Cross-site scripting** is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users. Examples of such code include html code and client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls.

CYBER LAUNDERING

Cyber laundering depends on the use of various types of transactions and financial service providers, ranging from wire transfers to e-money transactions. When laundering the proceeds of crime, criminals need to be quick and efficient. The perpetrators of cyber- crime tend to be well educated and technically competent individuals and the methods developed by them are quite complex and unconventional (Deccan Chronicle, 2018). Money laundering method involves cash withdrawals from ATM, as it allow criminals to avoid face to face contact with bank employees. International and national remittance systems and electronic money allow criminal to quickly and effortlessly launder cybercrime proceeds.

Cyber Security plays an important role in the ongoing development of information technology as well as internet services. The regulation of money transfers is currently limited and the internet offers offenders, the possibility of cheap and tax-free money transfers across borders. Current difficulties in the investigation of internet based money-laundering techniques often derive from the use of virtual currencies and the use of online casinos (Jyoti and Vijay, 2017). One of the key drivers in the development of virtual currencies was micro-payments. Unlike a real casino, large financial investments are not needed to establish online casinos. The regulations on online and offline casinos differ between countries.

Vulnerabilities of the financial system to cybercrime are to a large extent, associated with insufficient protection of banking information. Instead of attempting to attack a bank's system, this is usually equipped with strong protection (Michael Levi, 2002). Cyber criminals often favour those e-commerce portals and payment system where a great number of personal information and credit card data are being stored and processed. Cyber criminals also target at loopholes of mobile devices and the threats are growing faster than it does on personal computer. Mobile device holders tend to connect their devices to public free wireless network especially when travelling abroad. Remote transactions may be done by third parties which identify is not known to the banks or payment companies. The real identity of the persons conducting the distant transaction is hidden and thus the system may be used for performing illegal or cyber laundering activities.

SOLUTION TO PROTECT THE INFORMATION RESOURCES

The cyber criminals detect security holes which career criminals or even cyber-terrorist could use to attack them in future. a) Safeguarding and monitoring wireless access points, network access points, and network-attached devices by securing interfaces between agency-controlled and non-agency controlled or public networks, Standardizing authentication mechanisms in place for both users and equipment, Controlling users' access to information resources. b) To prevent insider attacks on agency networks access rights to files should be controlled and access should be granted only on as required for the performance of job duties.c) To prevent unauthorized access of information all hosts that are potential targets of DOS (Denial of Service) should be secured.

d) Authentic programs should be installed with Trojan scan Programs. e) To prevent against exploitation: Periodic scanning for spyware, adware and bots (software robots) shall be conducted with anti-spyware programs that detect these malicious programs. Provision of security awareness training to personnel on an annual basis that, in part, cautions against downloading software programs from the Internet without appropriate agency approval

CONCLUSION

Technology is always a double edged sword and it can be used for good or bad. At present our society is dependent more on technology. crime based on electronic offences are bound to increase and the law makers have to go the extra mile compared to the fraudsters to keep them at bay. An effective anti-cybercrime strategy consists of a series of legal, technical, organizational and informational activities, with the role of each of these activities being neither primary nor secondary. Nation builders, law makers and financial administrators have always taken persistent efforts to curb the evil of cyber laundering and all sorts of illegally earned income.

REFERENCES

1) *Animesh Sarmah, Roshmi Sarmah and Amlan Jyoti Baruah. (2017), " A brief study on Cyber Crime and Cyber Law's of India, Volume 04, Issue 06.*
2) *Deccan Chronicle, (2018),Cybercrime, available at: https://www.deccanchronicle.com/nation/crime/200718/indias-cybercrime-scenario-ground-situation-alarming.html*
3) *DOJ, Press Release, July 20, (2017), available at https://www.justice.gov/opa/pr/alphabay-largest-online-darkmarket-shut-down*
4) *http://www.ultrascan-agi.com/public_html/html/pdf_files/pre-release-419_fraud_statistics_2013-july-10-2014*
5) *Information Technology Act 2000, India, available at: http://www.mit.gov.in/itbill.asp (last visited on March 7, 2019*
6) *Juneed Iqbal and Bilal Maqbool Beigh. (2017), "Cybercrime in India: Trends and Challenges", International journal of innovations & advancement in computer science, IJIACS, vol 6, issue 12.*
7) *Jyoti Rattan and Vijay Rattan. (2017), "Cyber Laws & Information Technology" 47 Bharat law publishing, Calcutta, 6th edn.*
8) *K. Chethan. (2017), "One cybercrime in India every 10 minutes - Times of India," The Times of India, 22- Jul.*
9) *Leukfeldt, E. R., Kleemans, E. R., and Stol, W. P. (2016), "From low-tech locals to high-tech specialists. A typology of phishing networks", Crime, Law and Social Change. (in press)*
10) *Michael Levi. (2002), "Money Laundering and Its Regulation", Annals*

of the American Academy of Political and Social Science, Vol. 582, pp. 181-194.

11) *Nidhi Arya. (2019), "Cyber Crime Scenario in India and Judicial Response" Punjab, International Journal of Trend in Scientific Research and Development (IJTSRD), Volume 3, |Issue 4, Page: 1108.*
12) *Soudijn, M. R. J., and Zegers, B. C. H. T. (2012). "Cybercrime and Virtual offender convergence settings and Trends in Organized Crime", 15(2-3), pages 111-129.*
13) *Syed Azhar Hussain Shah, Syed Akhter Hussain Shah and Sajawal Khan. (2015), "Governance of Money Laundering: An Application of the Principal-agent Model" The Pakistan Development Review, Vol. 45, No. 4.*