MISERABLE IMPACTS OF CYBERCRIMES ON INDIAN BANKS A SOCIO-LEGAL COMPARATIVE STUDY OF INDIA, USA & UK

Apurv Banerjee[1] and Maryam Ishrat Beg[2]*
[1,2] Manipal University Jaipur
*Corresponding Author: maryam.pari75@gmail.com

ABSTRACT

Cyber technology made life easy for humans. But it also becomes easy for criminals to commit fraud with the help of this technology. In a few recent years, cybercrimes swiftly increased and drawn the attention of criminologists as well as this subject is becoming popular among research scholars also. The thing to be noticed here is that 80% of the cybercrimes take place due to the greed of money-making and this tendency of the criminals putting a serious challenge before the financial institutions. Among the financial institutions' bank is the institution which is targeted mostly by the criminals, the reason is that bank is the only place where the criminal can get the bulk of the money in one place. Cybercrimes are a serious threat to the whole world and it will not be incorrect to say that cybercrimes in today's world emerged as a global problem as well as a global challenge. The nature of these crimes makes them very hard to access these crimes and it makes it very tough to prevent these crimes. Because a criminal who commits cybercrimes is well –versed in the cyber technology and come out every time with innovative plans to commit a crime and in the meantime when a cybercrime is detected and the nature of cybercrimes understood the cybercriminals find out more typical ways to commit cybercrimes. Even the countries considered best in cybersecurity find it difficult to counter cybercrimes. So it is not hard to access the conditions of countries that are not having adequate resources to counter cybercrimes. This article presents the conditions of nations like India by comparing it with some of the countries which are considered topmost countries in cybersecurity like the United States of America and the United Kingdom.

***Keywords**: Bank, cybercrimes, data, financial, legislation*

Introduction

If a person loses money due to banking fraud or any cyber-attack due to which a financial institution fails to protect the money of a person. Then it is not only financial loss but also the loss of one's fundamental right as it is a breach of the right to privacy of a person. Where a bank fails to protect the personal data of an individual which is related to his financial privacy then it is an infringement of one's fundamental right as provided in Article 21 of the Indian constitution as in the case of K.S. Puttaswamy v. Union of India[1]-in this case, it was observed by the court that the right to privacy is the intrinsic part of Article 21 of the Indian Constitution. So personal and sensitive data of an individual must be protected..Unfortunately in India still there is no Act or law which separately deals with data Protection. In the year 2006,the Personal Data Protection Bill was first acquainted in Parliament after that in July 2017, the Ministry of Electronics and Information Technology established a committee to analyse in respect of data protection. Under the chairmanship of retired Supreme Court Judge Justice B.N.Srikrishna. Inthe year 2108 and in July the committee submitted a draft of the Personal Data Protection Bill 2018[2] cabinet ministry approved the bill on 4 December 2019 as Data Protection Bill 2019.This bill in Lok Sabha was tabled on 11 December 2019. Joint Parliamentary Committee analyzed the bill in March 2020. It doesn't mean that India doesn't at all have any legislation in this respect under the IT Act 2000 amended in the year 2008.[3]In the amendment act, there are provisions like Section 43A which deals with compensation in case of failure to protect data, and Section 72 provides for breach of confidentiality and breach of privacy Section 72 A covers Punishment for disclosure of the information in breach of lawful contract. The Information Technology (Reasonable Security and Procedures and Sensitive Personal Data and Information) Rules 2011[4]defines the 'sensitive personal data; which also includes the information regarding pieces of information such as bank account or credit card details and it also includes any kind of biometric information.

Introduction of Related Terms

Bank

There are different beliefs about the origin of the word "Bank". Some of the authorities

beliefs that the word " Bank " is derived from the word "Bangus" or "Banque" or "Bangue", which means a bench.

There are certain other beliefs also that the word "Bank" is derived from the German word "Back" the meaning of this word is joint-stock fund. In the Italian language, the word bank is known as "Banco". In the French language, the word bank is called "Banke" in English it is the word "Bank" and in Hindi, the same word "Bank" is used.

Banker

Banker is a person who is in the employment of any bank may be an executive or an official of the bank or a person who deposit money of the customers or engaged in the business of taking or receiving money from the customers and he has to return it in case it is demanded by the customers

In Oulton vs German Sav.& L.Soc[5]-the court was of the view that: The banking business is kind of a business where bank deposits money and the depositors when requires the money can draw it for any need. further, the functions of the banks got extended and banks also provide the loan on securities may issue currency and also can perform the task of exchanging. so the bank performs any of these functions or all of these functions. But even bank is restricted to perform any of these functions it will be considered as a bank with a point of view of commerce.

Internet Banking

Internet banking which is also known by various other names like online banking or web banking it is a kind of b system by which payments are made electronically by which a customer of the bank or any financial institution can make transactions through the website of the bank or the financial institution. System of Internet banking is connected with the or it is the part of the core banking which is different from branch banking which is a traditional style of banking.

Medium of Internet Banking

ATM

ATM which is known as Automated Teller Machine and also known as Cashpoint is a machine that is an electronic telecommunication device. Through this machine, a customer can make financial transactions with financial institutions. A customer can deposit or withdraw the cash or can transfer funds or can get account information. So there is no need for interaction with the bank staff. ATM is invented by John Shepherd Barron.

Debit Card

Debit Card which is also known by various other names such as bank cards or plastic cards or check cards is a plastic card for payment that can be used in place of cash when a customer makes a purchase. While making a transaction the money is transferred immediately and directly from the cardholder's bank account.

Credit Card

A credit card is a kind of a facility that is provided to the user or the cardholder for making payment to the merchant for goods and services. This card is a promise by the cardholder to the card issuer (which is usually a bank) to pay them for the amount and the other agreed charges.

ATM Cards

ATM cards are those cards which are used in automated teller machine. A customer through these cards can make various kinds of transactions like cash withdrawal, or getting the information of accounts and certain other types of transactions.

Direct Banking

Direct Banks are those banks that are without any branch network. In this kind of banking, the services are provided by distance through online banking and telephone banking or by an independent banking agent network and its services can also be accessed by the ATM or mail or mobile. The good thing about direct banking is that it reduces the cost of maintaining the branch and it also makes transactions faster.

Banking through Mobile

Banking through mobile is prevalent in today's moderns banking it is a service provided by the bank or any financial institution that allows customers to make transactions with remote areas using the devices like mobile or tablet. Generally, mobile banking takes place in a

software called an app. Banking through mobile is provided on a 24-hour basis. There are certain restrictions on mobile banking like which account can be accessed through mobile banking or amount can only be withdrawn up to a certain amount etc.

Cyber Crimes

Cybercrime is a computer-based crime that needs a computer and a network. The computer is used either to commit the crime or any computer may be the target of the crime. A person or a company or any financial institution can be the target of cybercrime.

Financial Cyber Crimes in Banks

Finacial cyber crimes in banks are digital wrongdoing and following things like PC or a network or a system of a bank may be the target of the cyberattack.

Results

The study reveals that on all the fronts India is lagging in cybersecurity whether it is in technical aspects or legislative aspects even the social approach of our country is pathetic about cybercrimes. The banking system of India is clueless as well as lazy and reluctant to take action on cyber crimes in comparison to countries like the United States of America where banks are investing large amounts to protect their country from financial cyber frauds. Even their approach towards cybercrime is so cautious that they have enacted legislation at the federal as well as state-level and they are swift at making required legislation when there is an urgent need to do so. This shows how prompt and cautious the USA is regarding their cybersecurity and the countries like England are though smaller than India but having better cybersecurity and adequate legislation and they are working constantly over their laws as per need of time and circumstances. It shows that cybersecurity is not only a priority in their countries but they are prepared and keep on preparing themselves to combat cybercrimes as they understand the seriousness of cyber offenses. So the study puts light on the pathetic conditions of India and the urgency to take action in this regard.

Discussion

In India, the concept of online banking took a long time to establish. The social reason for this is that Indians people are traditional by thinking so it took a long time to believe that online transactions are safe. The present government is also making every possible effort to promote digitalization in India but still at the rural level it will take time to establish in cities it is popular now. But things are not so easy as it looks the advancement of technology also advanced the way of committing cybercrimes and the fact is that it hampering the belief of the people from the online transactions. The concept of online banking came to India from developed countries like the USA or UK. These systems of electronic payments needs time to settle down as Indians are still learning to cope up with this system. There are many reasons for these people are not so well-versed in computers or with cyber technology to understand what exactly is going on. Eventhey are unaware of the modes in which cybercrimes are committed. The concept of online banking transactions became popular in the late 1980s in the United States of America. In India, online banking arrived in the late 1990s. Among Indian Banks, ICICI was the first bank to provide online banking to its customers in the year 1996. But online banking was established in the year 1999 in India.But now in India, it is gaining rapid growth and popularity and it is expected that India reaches 150 million online banking users by the year 2020. But as we discussed earlier that cyber technology has given rise to the cybercrimes also.[6] In India first ATM card fraud busted when a gang-related with digital wrongdoing. Police held a 22-year aged boy Deepak Prem Manwani who was held by police at the time when he was breaking into an ATM. As per the police report at the time he was caught he has with him Rs 2.5 lakhs that he received by knocking two ATMs in Chennai. According to a report, titled "ENCAHSING ON DIGITAL: Financial. Services in 2020". The report is drafted by Facebook and the Boston Consulting Group. After USA India is the second country to face most of the cyber-attacks. India constantly facing major or minor cyber attacks like two persons who were held in Mumbai as they

were involved in malafied activities related to money transfer from the bank accounts of many people by getting their SIM card details by dishonest means. They also hacked the accounts of many companies and nearly transferred 4 crore rupees from various accounts. In a major attack on cosmos bank, the hackers hacked the ATM server of the bank and took details of many debit card and visa owners they wiped out money and transferred it to a Hong Kong situated bank by hacking the server of cosmos bank on August 2018 nearly 94 crore rupees siphoned off from Pune branch of cosmos bank.In Kolkata, the ATM server is attacked this incident, the hackers wiped off nearly 20 lakh rupees and 50 persons got effected by the attack it was believed that the attackers had details of more than 300 ATM users. From April 2017 to January 2018 over 22,000 websites were hacked and according to the report of the Computer Emergency Response team more than 493 websites were affected by malware which includes 114 websites run by the government. The intent behind these attacks is together details of the users of the network. According to an article published in Economic Times during the year, 2017-18 cases of banking cyber frauds estimated at Rs 109.6 crore took place and nearly 2059 cases were reported whereas it was Rs 42.3 crore and 1371 cases of cybercrimes were reported during the year 2016-2017 the amount almost doubled within a year. There are many reasons in India that the banking cyber frauds are increasing constantly in India first and foremost reason is that the banks have a negative approach towards the protection of cyber frauds taking place in the Indian banks, for instance, banks are reluctant to report cyber frauds as it will lead to the downfall of their goodwill and this is going to badly affect their banking business as people avoid to deposit their money in such banks where these banking cyber frauds are taking place. According to the Economic Times banks are reluctant to report fraud but for a strong system, it is needed that the bank's industry should be prompt in reporting and in taking action. Following the money, the trail is not possible once it crosses borders said Arundhati Bhattacharya, who is a former chairman of the State Bank of India. Rajnish Kumar, Chairman State Bank of India said during his interview to the Economic Times "Underreporting of cyber frauds is not acceptable timely reporting is very important because I am only looking at my bank, but if another bank is hit by a cyber fraud and it is reported in time, it can be analyzed swiftly and such future frauds can be avoided. If there is a delay in reporting we miss the opportunity". Many cybercrimes in the bank are taking place like Hacking, Phishing, Vishing, or E-mail spoofing, Spamming, Denial of
service or Advanced Persistent Threat, and ATM Skimming and Point of Sale taking place in Indian banks and the Indian banks are careless in dealing with such kind of cyber frauds. The internet is the medium of interconnectivity and the cybercriminal takes advantage of this feature of the internet so by doing so criminals target the very foundation of our society. The customer of banks feel anxiety, worry, anger, outrage depressed or annoyed and cheated a few of them blame themselves to be attacked, and very few number of people things that it will not happen to them. It is quite disheartening that nearly 80 % of the people things that cybercriminals can not be brought to justice. Many of the persons are of the view that they going to change their behavior if any incident like that takes place in their life only a few of them report such incidents so negative emotional impact can be seen in the society related to the cybercrimes. A single successful cyberattack has a far-reaching impact on an individual like financial losses and loss of confidence and trust and so on. Another emotional factor that is relevant here is fear and it may lead to stress, and unrealistic public fear of crime and danger even without the presence of such fear. Sometimes people take these risks voluntarily by doing risky online activities some times they took the risk because they are unfamiliar or lack an understanding of the risk involved or of the consequences and sometimes due to lack of protection. Members of the public or experts both might get confused about facts due to their judgment or interpretation because the perception of the facts are depending on these variables. Many people became victim of mistrust as most of them think that they may be any time scammed or defrauded online. Policymakers can not achieve success without

considering these realities and mental traits. Generally, environment and personal factors together posing threats in the mind of the people. Appraisal of threat also depends upon how susceptible one feels to a danger decides the extent of the safety level one is going to use. Instead of understanding the nature of cybercrimes, people are of the view that there is very little they can do about these attacks. Know there are two kinds of mental approaches people have towards life one is that whatever is happening is the result of their activities. Whereas some people beliefs that other factors like luck or action of other people are also responsible for their failure or success so this kind of person despite taking their protective measures depends upon the Internet providers and government to provide safety measures. So we can say that attitudes, intentions, or behavioral changes control the risks. An individual who thinks or judges himself capable enough to deal with potential threats neither fear nor avoids threats. Whereas the persons who found themselves unable to counter the potential threat then they become stressed and start avoiding threats because they judge themselves that they are not having the necessary skills or knowledge and therefore they start avoiding to act or to take any protective impact.

Banking Cyber frauds

Bank is the institution got the biggest advantage of information technology and use d information technology very largely to provide the service to its customers. But with the rapid expansion of information technology and a new form of crime which is known as cybercrime is emerged as a new branch of crime. As the banks taking the biggest advantage of computers or internet technology there are also facing the biggest disadvantages of the technology. According to research conducted by Juniper Research in the year 2016, it is estimated that the global cost of cybercrimes could be 2.1 trillion by 2019. These data which are shown in the studies conducted are just indicative in reality the loss of money is much higher than these estimations. These kinds of digital assaults are increasing in India and the world swiftly. These digital violations or wrongdoings can be classified into the following :

Hacking – Hacking is an effort to exploit a computer system or an attempt to exploit a private network in a computer or we can call it unauthorized access or an effort to control a computer network security system for any illegal or illicit purpose. In the IT amendment Act under section 43, there is a penalty for hacking further section 66 lays down that if any person commits any act as specified under section 66 of the IT Act then he shall be punished with imprisonment which may be extended to three years or there will be fine which may extend to five lakh rupees. In the USAthe hacking is defined in the[7] Computer Fraud Act and Abuse Act under section 1030 18 U.S.C. In the UK hacking is defined in the Computer Misuse Act.In the case of *State Bank of India v. Chander Kalani &Ors*.[8]The Telecom Disputes Settlement and Appellant Tribunal New Delhi was adjudicating a dispute about the alleged hacking of the complainant's email ID address and leak of confidential information about the complainant's bank account. The complainant alleged that the bank was negligent in disclosing details of the complainant's bank account by responding to fake emails and was, therefore, liable to pay the complainant compensation under section 43A of the IT Act. In this case, the TDSAT held that." on a careful reading of Section 43A, it is clear that negligence in implementing and maintaining reasonable security practices and procedures alone creates a liability to pay damages or compensation under Section 43A.

Phishing

Phishing is a fraudulent practice of sending emails pretending to be sent from reputable companies to induce a person or persons to reveal their personal information like passwords and credit card numbers etc. Phishing is a punishable offense under Section 43 of the IT Act. In US Phishing is covered under many state laws but there is no single federal law that directly criminalizes phishing. In the UK Phishing conviction can result in a year or more prison though law differs but still five years prison can be possible. . In the case of *Umashankar Sivasubramainam v. ICICI Bank*[9]The Adjudicating officer deciding a

case under the IT Act in Chennai was deciding a dispute about phishing In the case the complainant received a fake security update he assumed it to be of ICICI so he shared his details of the bank account as a result certain amount was debited from his account Adjudicating officer held the bank responsible under Section 43A and held the bank fail to exercise due diligence by not preventing "unauthorized access". On appeal, the TDSAT was of the view that " The Section 43A was inserted on later that so this Section will not be applicable the relevant Section is 43(g) in this case. It was held that the bank is responsible to pay damages as the bank failed to prove in defense that sufficient security measures are taken even the bank fails to secure its e-mail system from misuse.

Vishing – The term vishing means a fraudulent practice in which phone calls are made or voice messages are left which purports to be from banks or reputed companies etc. The basic aim is to induce individuals to disclose personal information's like details of the bank or the credit card number. This word vishing is a combination of two words 'Voice' and 'Phishing'. Fishers use internet telephone service in place of email or regular phone calls or fake websites as used by phishers generally

Spamming – Spamming is the sending of the message which is Unsolicited Commercial Emails these messages are sent indiscriminately to many internet users. From cybercrime, spamming is used to spread computer viruses or Trojan horses and many other kinds of malicious spams. The aim is to commit identity theft or even something worse. As of now, there is no present law that exists in India for spam the old and traditional law of torts like the principle of trespass to goods or the law of nuisance as specified in the law of torts are applicable. Section 43 of the Information technology also covers spamming.. Section 43 of the Information technology also covers spamming. In the United Kingdom the law is known as Privacy and Electronic Communications (EC Directive) Regulations 2003.

Denial of Service attack- DOS or denial of service attack is a kind of an attack where the object is to shut down the machine or any network by DOS attack the network or machine attack is made inaccessible to the users. In this kind of attack, the target is flooded with traffic or by sending information that triggers a crash, Dos attacks are covered under the Section 43(e), (f) (g) of the Information Technology Act 2008.[10] In the United Kingdom, the DOS attack is covered under The Computer Misuse Act. 1990. In the United States of America, the DOS attack is dealt with under the Computer Fraud and Abuse Act.

Skimming- Skimming is a kind of a cybercrime in which identity thieves by an illegal practice capture credit card information from a cardholder. The person who commit such fraud is called a skimmer. The fraudster often uses a device called a skimming device. These devices are smaller than a deck of cards. These devices are generally fixed in places like card reader entry slot or speaker area or ATM keyboard area or maybe in the areas like light diffuser area or ATM side fascia etc. Generally, cameras are positioned in such a way to capture PINs. If the number is captured then the electronic data is put into a fraudulent card and then used to withdraw the money from the help of that captured PIN.. identity theft includes both theft and fraud so along with the information technology act the provisions of the Indian Penal Code is also applicable like Section 465 of the IPC for covering forgery, or making or preparing false document Section 465, forgery for purpose of cheating Section 468 Under the Information Technology Act the Skimming is dealt under section 43 and a fraudster who commits such kind of the crime shall be punished according to the section 66 of the information technology act. In the United Kingdom, credit cards are regulated by laws like the Consumer Credit Act. There are some federal laws for the card frauds like 15 U.S.C. Section 1644 (federal fraudulent credit card, 15 U.S.C Section 1693 (federal fraudulent debit card). In states like Alabama and California,[11] there are separate codes in the USA.

Conclusion

The research reveals the incompatibility of India to counter cybercrimes and the hazardous effects of the cyber crimes on banking institutions which is causing economic loss to

India. The response of the banking institution is very negative which increased the confidence of the cybercriminals to commit constant financial cybercrimes. Even the data protection agencies or cyber cells look helpless to combat cybercrimes. Those persons who become a victim of cyberfraud accept it as their destiny and those who are not yet become a victim despite knowing the seriousness of these crimes are ignorant and lack information. So it is the approach which is needed to be improved first because we need to fight back and we are lucky that we have examples of the countries doing well in this area we need to learn and follow these countries. Our criminologist need to make intense researches to combat these crimes and banks needs to invest money to prevent the financial cyber crimes because one major cyberattack can cause the bank to be bankrupt. Government needs to take prompt actions to protect against the damage to the economy by these types of financial cybercrimes and people need to increase there awareness so that they can protect themselves from these cybercrimes by the time there is no strong protection in India against these kinds of cybercrimes and the legislation needed to be adequate and there should be prompt legislation and amendments required in reference of this serious problem.

References

1. Writ Petition (Civil) No 494 of 2012 ,SC
2. PDP Bill Introduced by Ravi Shankar Prasad in Lok Sabha.
3. Indian Parliament in the December 2008 passed IT Amendment Act.
4. Notified by Government of India on April 11,2011
5. Wall 109 ,118, 2IL .ED.618
6. Www.legalserviceindia.com
7. Bill was enacted in year 1986 added in Comprehensive crime control Act 1984
8. Appeal No .13 of 2015 (M.A.No 282 of 2017)
9. Petition No. 2462 of 2008
10. Michael Colvin introduced the Act .Commenced from 29 August 1990.
11. California Penal Code Section 484gPC.