"Cyber Crime in Banking Sector*[1]"

-Sanchi Agrawal

Abstract

Online banking or e-banking refers to the banking facility through information and communication technology. Traditionally, banking required a customer to stand in a long queue even to withdraw his money or to perform other ancillary functions. Now banking facility is available 24×7 through ATMs (Automated Teller Machines), internet banking, transfer through NEFT and RTGS etc., which has narrowed down the gap between the bank and the customer. E-banking is not only limited to banking facility through computer related systems. In the modern era, with the increase of users of smartphones e-banking covers mobile banking also. Because of liberalization, privatization and globalization it became necessary for the banks to start with e-banking facility.

The paper will provide an introduction to the concept of e-banking and its advantages in India. Further the author will provide statistics of the increase in use of e-banking services in India. The paper shall also highlight the role of Reserve Bank of India in strengthening internet banking.

The paper shall then delve into the drawbacks of e-banking by explaining various cyber-crimes related to banking focusing on Information Technology Act, 2000 with the help of statistics on cyber-crime reported in the past few years. Cyber-crimes are crimes related to computer, computer resource or computer network or communication device. Some of the cyber-crimes in banking sector are phishing, hacking, skimming, pharming etc.

Lastly, the author shall highlight the role of Cyber Appellate Authority in combating cyber-crime in banking sector. The liability of both the bank and the customer depending upon the facts and circumstances of the case shall also be discussed. Finally the author shall suggest the safeguards a customer and a bank should undertake while dealing electronically.

Keywords: e-banking, cyber-crime, IT Act, 2000, communication device, computer resource

[1] Sanchi Agrawal, 5th Year student, BA LLB(H), Amity Law School, Delhi (GGSIPU)

1. Introduction

Economy is one of the pillars which defines about the progress and growth of a nation. Banking sector is considered as the backbone of the economy. For our day-to-day transactions we enter into monetary transactions in the form of cash payments, cheques or demand drafts. However, this trend has paved the way to a modern system of payment in the form of swiping of debit cards or credit cards. On the recommendation of the Committee on Financial System (Narasimham Committee) 1991-1998[2], information and technology in banking sector was used.

On one hand, technology has created advantage for banks and financial institutions but on the other hand, there have been risks involved in it also. Technology risks not only have a direct impact on a bank as operational risks but can also exacerbate other risks like credit risks and market risks. Given the increasing reliance of customers on electronic delivery channels to conduct transactions, any security related issues have the potential to undermine public confidence in the use of e-banking channels and lead to reputation risks to the banks. Inadequate technology implementation can also induce strategic risk in terms of strategic decision making based on inaccurate data/information.[3]

Banking sector has witnessed expansion of its services and strives to provide better customer facility through technology but cyber-crime remains an issue. Information which is available online is highly susceptible to be attacked by cyber criminals.[4] Cyber-crimes result in huge monetary losses which are incurred not only by the customer but by the banks also which affects economy of a nation. Non-monetary cyber-crime occurs when viruses are created

[2] The Narsimham Committee was first set up in 1991 under the chairmanship of Mr. M. Narasimham the then 13th governor of RBI. Since all of its recommendations were not implemented second committee in 1998 was set up.

[3] RBI Guidelines on Information Security, Electronic Banking, Technology Risk management and Cyber Frauds, 2012.

[4] Soni RR and Soni Neena, *An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks*, Vol. 2(7), 22-27, July (2013), Research Journal of Management Sciences, Available online at: www.isca.in

and distributed on other computers or confidential business information is posted on Internet. The most common of it is phishing and pharming.

2. Concept Of E-Banking

Electronic Banking or e-banking refers to a system where banking activities are carried out using informational and computer technology over human resource. In comparison to traditional banking services, in e-banking there is no physical interaction between the bank and the customers. E-banking is the delivery of bank's information and services by banks to customers via different delivery platforms that can be used with different terminal devices such as personal computer and a mobile phone with browser or desktop software, telephone or digital television.[5]

The first initiative in the area of bank computerization was stemmed out of two successive Committees on Computerization (Rangarajan Committee).[6] The first committee was set up in 1984 which drew the blueprint for the mechanization and computerization in banking industry. The second Committee was set up in 1989 which paved the way for integrated use of telecommunications and computers for applying fully the technological breakthroughs to the banking operations. The focus shifted from the use of Advanced Ledger Posting Machines (ALPMs) for limited computerization to full computerization at branches and to integration of the branches.[7] Till 1989, banks in India had 4776 ALPMs at the branch level, over 2000 programmers/ systems personnel and over 12000 Data Entry Terminal Operators.[8]

[5] *Daniel, E.* (1999), Provision of electronic banking in the UK and the Republic of Ireland, International Journal of Bank Marketing, Vol. 17, No. 2, pp. 72-82.

[6] Committees on Computerization < https://www.rbi.org.in/Scripts/PublicationsView.aspx?id=162> accessed 24th August, 2015.

[7] *Dr. B R Sharma and Dr. R P Nainta*, Banking Law & Negotiable Instruments Act, 4th Edn, Allahabad Law Agency, p 183.

[8] *Talwar S P*, (1999), National Seminar on Computer Related Crime, Inaugural address by Shri S P Talwar, Deputy Governor, Reserve Bank of India, February 24, 1999.

The RBI constituted a Working Group on internet Banking. Based on the notion of access to the banking products and services, the group divided internet banking into three systems.[9]

(a) Informational System

This system requires banks to provide information about interest rates, loan schemes, branch locations etc. to the customers. The customer can download various types of application as per the requirements. Also customers are not required to reveal their identity and there is no realistic chance of any unauthorized person getting into the production system of the bank.[10]

(b) Communicative System

This system provides information to the customer about his account balance, transaction details etc. The customers can seek the information after authentication and logging in through the passwords.[11]

(c) Transactional System

In this system a bank allows its customers to undertake transactions through its system and they are directly uploaded to the customer's account. There is bi-directional transaction that takes place between the bank and the customer and between the customer and the third party. This system is secured through security mechanisms like http and https.

E-banking is also known as Cyber Banking, Home Banking and Virtual Banking. E-banking includes Internet Banking, Mobile Banking, RTGS, ATMs, Credit Cards, Debit Cards, Smart Cards etc.[12] Some of the forms of E-banking are explained below:

(1) Automated Teller Machines (ATMs)

An ATM is a device which is located on or off the bank's premises. It enables a customer to withdraw cash, obtain statement of law few transactions in his account, statement withdrawal and to transfer funds from one account to another. A person can withdraw cash 24x7 from ATMs subject to the limit provided. This system is also known as 'Any Time Money' or 'Anywhere Money'.[13] To have access of ATM a person must have an ATM card.

---

[9] Reserve Bank of India, *Report on Internet Banking,* https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=243#ch2, last accessed 24th October, 2015.

[10] *Ibid*

[11] *Ibid*

[12] Dheenadhayalan V., *Automation of Banking sector in India*, Yojana, February, (2010) p.32.

[13] Dr. Roshan Lal & Dr. Rajni Saluja, *E-Banking: The Indian Scenario*,December (2012), Vol (1)(4), http://indianresearchjournals.com/pdf/APJMMR/2012/December/2.pdf accessed on 24th August, 2015.

The ATM card is inserted into the machine and the client is required to enter a personal identification number (PIN). PIN is the numeric password which is separately mailed or handed over or sent by post to the customer by the bank while issuing the card. Most of the banks require that customers change their PIN on after first use. Banks' also send alerts to the customers not to disclose their PIN to anybody, including to bank officials. Customers should change the PIN at regular intervals. The transactions carried out using ATM machines are quite easy.[14]

There are two types of ATMs, one, exterior ATMs which are located in shopping centers, railway stations, airports etc. and second, interior ATMs which are located within the bank premises.[15] The limits on cash withdrawal at ATMs and for purchase of goods and services are decided by the issuer bank. Nowadays a customer can use ATM of another bank also to withdraw cash. However, in case of such withdrawal at other bank's ATM there is a limit of cash withdrawal.

(2) Real Time Gross Settlement System (RTGS)

RTGS is a system where funds are transferred from one bank to another on 'real time' and on 'gross basis'. RTGS transactions are carried through either interbank or it can be between customers through bank accounts.[16] 'Real Time' means the processing of instructions at the time they are received rather than at some later time; 'Gross Settlement' means the settlement of funds transfer instructions occurs individually (on an instruction by instruction basis). The transactions are settled individually in RTGS.[17]

RTGS transactions are processed throughout the business hours of banks. The timings of business hours at different bank branches are decided by the banks on their own terms and policies. Generally RTGS transactions for customers are available from 9:00 hours to 16:30 hours on weekdays and from 9:00 to 14:00 hours on Saturdays where settlement is to be done at the RBI end. [18]

[14] https://rbi.org.in/scripts , last visited on 18th Feb, 2016.
[15] *Dr. B R Sharma and Dr. R P Nainta*, Banking Law & Negotiable Instruments Act, 4th Edn, Allahabad Law Agency, p 199.
[16] N Jamaluddin, '*E-Banking: Challenges and Opportunities in India'* (Proceedings of 23rd International Business Research Conference 18 - 20 November, 2013, Marriott Hotel, Melbourne, Australia)
[17] https://rbi.org.in/Scripts/FAQView.aspx?Id=65 , last visited on 18th February, 2016
[18] *Ibid*

In the RTGS system mainly large value transactions are processed. The minimum amount that can be remitted through RTGS is Rs. 2 Lakh. Only minimum limit is provided for payment transaction through RBI settlement. No maximum limit is prescribed for RTGS transactions.

(3) Credit card and Debit Card

Banks issue debit cards that are linked to a customer's bank account. Debit Cards can be used to transfer funds only for domestic purposes from one person to another person.[19] At present, a customer can use his Debit Card to withdraw money, know the monthly statement etc by using another bank's ATM, not being the ATM of the bank which issued such debit card. In case a customer transacts through an ATM of another bank from his savings bank account using his debit card then he is not charged by his/her bank till five transactions which includes both non-financial & financial transactions in a month. However, this five free transaction limit for transactions done at ATM of another bank is restricted from to three transactions in six metro cities which includes, Delhi, Mumbai, Chennai, Bengaluru, Kolkata and Hyderabad.

Like Debit cards, it is banks/other entities permitted by RBI issue credit cards to a customer. A Credit card has dimension of about 8.5 cm by 5.5 cm. It is a small rectangular shape plastic card bearing the name of the holder of the card i.e., the customer and the account number is printed over it. In addition, the date up to which the card is valid will also be embossed and a specimen signature panel on the revere. A card holder is also given the list of shops and establishments in each city where the card will be accepted in lieu of cash. The limit up to which the card holder can make purchases in a month is also informed to the card holder, this limit is called card limit.[20]

(4) Internet Banking

Internet Banking is a result of computerization of banking sector. It was necessary for the banks to open up internet banking activities because of cut-throat competition. Furthermore,

[19] Reserve Bank of India https://rbi.org.in/scripts/FAQView.aspx?Id=103 accessed on 15th September, 2015.
[20] *Supra* note 35 at pg 201.

Internet banking facility being available at all time has created an advantage for the customers. There has been a paradigm shift from 'bricks and mortar' to 'click and mortar' in the banking sector. The first bank to start with internet banking facility was ICICI followed by IndusInd Bank and HDFC Bank respectively in 1999.[21] Internet Banking is beneficial because it is convenient and easy to do banking business from home or at office desk. One can avoid standing in long queues or delays.

Simply by logging using User ID and Password one can experience Internet Banking. With a click on the internet a customer can check his account statement, transfer funds from one account to another, open FD (fixed deposit), pay electricity or telephone bills or pay rent, can recharge his/her postpaid or prepaid bills etc. [22]

(5) Mobile Banking

The importance of mobile phones for providing banking services has increased. We have become dependent on our mobile phones these days. Because of the growth of mobile phone subscribers in India, banking services have been extended for the customers to be availed through their mobile phones. Mobile banking is when transactions are carried out using a mobile phone by the customers that involve credit or debit to their accounts. In 2014 RBI had set up a Committee on Mobile Banking under the Chairmanship of B Sambamurthy. The Committee is required to study the problems faced by the banks in providing mobile banking to the customers and to examine the options including the feasibility using encrypted SMS-based funds transfer.[23]

Mobile banking facility has witnessed tremendous growth in our country. In the financial year (2015-2016), mobile wallets overtook mobile banking in number of transactions. Mobile wallets transactions- from phone recharges to paying for cabs or shopping online- trebled to almost 400 million through April-November 2015. Mobile wallet system is there in Apps like Jugnoo, Ola, Uber, Mobikwik, Paytm etc.

[21] *Supra* note 29

[22] http://www.icicibank.com/Personal-Banking/insta-banking/internet-banking/index.page , last visited on 28th Feb, 2016.

[23] Harun R Khan, *Digital India: Emerging Challenges and Opportunities for the Banking Sector*, Federation of Indian Banks Association (2014)

It has been reported by Times of India that the number of transactions in mobile banking has more than doubled from 98 million to 265 million in first eight months in the fiscal year of 2014-2015. If the growth continues at such a rate then it is clear that mobile based transactions be it mobile wallet or mobile-banking transaction, will surpass cheque payment system in some months only. In the present scenario, mobile based transactions added up to 602 million i.e., 83% of the 723 million cheques cleared during April, 2015 to November, 2015. However, the proportion of m-banking was less than 30% till last year. Approximately Rs. 1.26 lakh crore was spent by a customer in 2015 through mobile payments that resulted in a growth of 87% in mobile payment volumes.[24]

If we look at the rise of E-banking it is clear that people have started using this facility ore in comparison to traditional for of banking as evident from the table below for transaction in April-November, 2015 (in millions).

	2014-2015	2015-2016
Cheques	793.1	729.3
Online payment RTGS	59.3	64.0
Retail Electronic Clearing	890.4	1922.3
Mobile Wallets	133.9	399.1
Mobile Banking	97.7	203.1

Source: RBI Payment System Indicators.

3. Cyber Crime: Types And Its Impact On Banking Sector

Neither crime nor cyber-crime has been defined in IPC or Information Technology Act, 2000 (hereinafter referred as IT Act), but only provides punishment for certain offences. The word 'cyber' is synonymous with computer, computer systems and computer network. Thus, it can be said that cyber-crime occurs when any illegal activity is committed using a computer or computer resource or computer network. Douglas and Loader have defined cyber-crime as a computer mediated activity which is conducted through global electronic

[24] Aparna Desikan, *Mobiles making India less cash conscious*, Times of India, 22nd February, 2016, pg 1.

networks that are either considered illicit or illegal by certain parties.[25] Cyber crimes have been classified into four categories by Wall. They are cyber-deceptions, cyber-violence, cyber-pornography and cyber-trespass.[26] The frauds in e-banking sector are covered under cyber-deception. Cyber-deception is further defined as an immoral activity which includes theft, credit card fraud, and intellectual property violations. Mostly frauds are committed because of two goals, one, to gain access to the user's account an steal his personal information and transfer funds from one account to another. Second is to undermine the image of the bank and block the bank server because so that the customer is unable to access his account.[27]

In terms of number of cybercrime incidents in ransom ware, identity theft and phishing attacks India has been ranked among the top 5 countries.[28] According to Global Economic Crime Survey 2014, conducted by PwC, cybercrime was one of the top economic crimes which was reported by various organizations across the world, including India.[29] National Crime Records Bureau (NCRB) reported that a total of 5,752 persons were arrested for committing cyber crimes during 2014 as compared to 3,301 persons arrested in 2013 registering 74.3% increase over the previous year. Uttar Pradesh (1,223) was reported with the maximum number of persons arrested under such crimes.[30]

Banking sector too has suffered an impact of cyber crimes. RBI has defined bank fraud has as, 'A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank'[31]

3.1 Cyber Crimes Related With Banking Sector

[25] Douglas, T., & Loader, B. D.*Cybercrime: Security and surveillance in the information age*: Routledge Publisher 13 April 2000

[26] Wall, *Cybercrimes and the Internet*, 4th Edn, Routledge, (2001)

[27] A R Raghavan & Latha Parthiban, *Effect of Cyber Crime on Bank's Finances*, Vol. 2(2) Feb 2014 p 173-178 < http://ijcrar.com/archive-6.php > accessed on 24th August, 2015.

[28] 2013 Norton Report, http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013 > accessed on 23rd September, 2015

[29] Current Fraud Trends in the Financial Sector, ASSOCHAM India, June 2015

[30] National Crime Records Bureau, < http://ncrb.gov.in/> , accessed on 1st October, 2015

[31] Reserve Bank of India, *Report of the Study Group on Large Value Bank Frauds*,1997

(1) **Hacking**

Hacking is a crime, which means an unauthorized access made by a person to cracking the systems or an attempt to bypass the security mechanisms, by hacking the banking sites or accounts of the customers. The Hacking is not defined in the amended IT Act, 2000[32]. But under Section 43(a) read with section 66 of Information Technology (Amendment) Act, 2008 and under Section 379 & 406 of Indian Penal Code, 1860, a hacker can be punished[33]. Before the 2008 Amendment Act, Hacking was punishable under Section 66 of the IT Act with upto three years of imprisonment or fine which may extend upto two lakh rupees, or both. If such crime is proved then for such hacking offence the accused is punished under IT Act, for imprisonment, which may extend to three years or with fine, which may be extended to five lakh rupees or both. Hacking offence is considered as a cognizable offence, it is also a bailable offence.

(2) **Credit Card Fraud**

There are many online credit card fraud are made when a customer use their credit card or debit card for any online payment, a person who had a mala fide intention use such cards detail and password by hacking and make misuse of it for online purchase for which the customers card used or hacked is suffered for such kind of attract or action of a fraud made by and evil[34]. The hacker can misuse the credit card by impersonating the credit card owner when electronic transactions are not secured.

(3) **Phishing or Identity Theft**

Phishing is a scam where Internet fraudsters request personal information from users online. These requests are most commonly in the form of an email from an organization with which one may or may not do business. In many cases, the email has been made to look exactly like a legitimate organization's email would appear complete with company logos and other convincing information[35]. The email usually states that the company needs to update personal information or that the account is about to become inactive, all in an effort to get

[32] Types of Cyber Crimes & Cyber Law in India, Available at http://www.csiindia.org/c/document_library/get_file?uuid=047c826d-171c-49dc-b71b-4b434c5919b6, Last visited (30/4/2015

[33] http://164.100.47.134/lsscommittee/Information%20Technology/15_Information_Technology_52.pdf

[34] Barkha Bhasin, Rama Mohan Ukkalam, Cyber law and Crimes, Edn 3rd, Asia Law House, pg. 7.

[35] http://indianexpress.com/article/cities/pune/onlinebankfraudagainwomandupedofrs35000/

the user to click the link to a site that only looks like the real thing. Phishing is only one of the numerous frauds on the Internet, attempting to trick individuals into separating with their cash. Phishing alludes to the receipt of spontaneous messages by customers of financial institutions, asking for them to enter their username, password or other individual data to access their account for some reason. Customers are directed to give a response to a mail and also directed to click on the link mentioned in the mail when they click on the given link for entering their information which were asked in the mail received by the fraudulent institutions of banking website, by such kind of activities customers thus they remain unaware that the fraud has happened with them. The fraudster then has admittance to the client's online financial balance available in the bank account and to the funds contained in that account by making the misuse of the detail received from the customer fraudulently[36].

In the case of *Umashankar Sivasubramanian* v. *ICICI Bank*,[37] the petitioner used to receive monthly bank account statement under the email ID of the bank, one day received a mail asking for his personal details, which he provided, after which his account was debited with Rs. 5 lakhs. Upon complaint, the bank said that it was a phishing mail against which he approached the adjudicating officer. In this case, the bank was held liable according to Section 43 and Section 85 of the IT Act, 2000, as it failed to establish due diligence and providing adequate checks and safeguards to prevent unauthorized access into the customer's account. The bank was directed to pay Rs. 12.5 lakhs.

In *National Association of Software and Services Companies* v. *Ajay Sood*[38], a reasoned order approving a settlement agreement between the plaintiff and the defendants in a case which dealt with the issue of 'phishing', wherein a decree of ` 16 lakhs was passed in favour of the plaintiffs. The plaintiff contended that the defendants were masquerading as NASSCOM, and were sending emails, in order to obtain personal data from various addresses, which they could then use for head-hunting, and they went on the website as if they were a premiere selection and recruitment firm. The suit was filed praying for a decree of permanent injunction restraining the defendants or any person acting under their authority from circulating fraudulent e-mails purportedly originating from the plaintiff of using the

[36] http://resources.infosecinstitute.com/modern-online-banking-cyber-crime/, Last visited (20/1/2015)
[37] Umashankar Sivasubramanian vs. ICICI Bank (Petition No. 2462 of 2008) Judgment Dated 12th April 2010
[38] 119(2005)DLT596, 2005(30)PTC437(Del)

trademark 'NASSCOM' or any other mark confusingly similar in relation to goods or services. A compromise application was filed before the court and the court while approving the settlement agreement observed that "in US an Act is proposed which, if passed, will add two crimes to the current federal law; It would criminalize the act of sending a phishing email regardless of whether any recipients of the email suffered any actual damages. It would criminalize the act of creating a phishing website regardless of whether any visitors to the website suffered any actual damages." The Hon'ble Judge further observed that "I find no legislation in India on 'phishing'. An act which amounts to phishing, under the Indian law would be a misrepresentation made in the course of trade leading to confusion as to the source and origin of the e-mail causing immense harm not only to the consumer but even the person whose name, identity or password is misused. It would also be an act of passing off as is affecting or tarnishing the image of the plaintiff, if an action is brought by the aggrieved party. Whether law should develop on the lines suggested by Robert Louis B Stevenson in his article noted above is left by this Court for future development in an appropriate case."

(4) **Keystroke Logging or Keylogging**

Key logging is a method by which fraudsters record actual keystrokes and mouse clicks. Key loggers are "Trojan" software programs that target computer's operating system and are "installed" via a virus. These can be particularly dangerous because the fraudster captures user ID and password, account number, and anything else that has been typed.

(5) **Viruses**

A virus is a program that infects an executable file and after infecting it causes the file to function in an unusual way. It propagates itself by attaching to executable files like application programs and operating system. Running the executable file may make new copies of the virus. On the other hand there are programs, that can copy themselves, called worms which do not alter or delete any file, but only multiply itself and send the copy to other computers from the victim's computer.[39]

(6) **Spyware**

Spyware is the number one way that online banking credentials are stolen and used for fraudulent activities. Spyware works by capturing information either on the computer, or

[39] *Kamika Seth*, Cyber Laws and Information Technology Age, Lexis Nexis publication, p 446.

while it is transmitted between the computer and websites. Often times, it is installed through fake "pop up" ads asking to download software. Industry standard Antivirus products detect and remove software of this type, usually by blocking the download and installation before it can infect the computer[40].

(7) **Watering hole**

"Watering hole" cyber fraud is considered to be a branch arising from phishing attacks. In watering hole a malicious code is injected onto public web pages of a website which is visited only by a small group of people. In a watering hole attack situation, when the victim visit the site injected with malicious code by attackers the information of such victim is then traced by the attacker. In phishing attack, victim himself gives away information innocently whereas in watering hole the attacker waits for the victim to visit the site. There can be an increase in watering hole incidents when there is more misuse and exploitation of zero-day vulnerabilities in various software programs like Adobe Flash Player or Google Chrome. Cyber criminals in watering hole use the kits available in black market to infect, inject and configure a website which may be new or updated to lure people to provide them details. The site which is to be used for an attack is usually hacked by the attackers' months before the actual attack. They use professional methods to perform such act. Therefore it becomes difficult for cyber-crime cells to locate such infected website. Watering hole is thus a method of surgical attack where the hackers aim to hit only certain specific group of people in the internet and in comparison to phishing it is less earsplitting.[41].

(8) **Credit Card Redirection and Pharming**

Pharming is linked with the words, 'farming' & 'phishing'. In Pharming a bank's URL is hijacked by the attackers in such a manner that when a customer log in to the bank website they are redirected to another website which is fake but looks like an original website of the bank. Pharming is done over Internet and Skimming is another method which occurs in ATMs.

(9) **DNS Cache Poisoning**

[40] http://indianexpress.com/article/cities/pune/cybercrimeinpuneunsecureddigitalindiadangerous/

[41] *Supra* Note 59

DNS servers are deployed in an organization's network to improve resolution response performance by caching previously obtained query results. Poisoning attacks against a DNS server are made by exploiting vulnerability in DNS software. That causes the server to incorrectly validate DNS responses that ensure that they're from an authoritative source. The server will end up caching incorrect entries locally, and serve them to other users that make the same request. Victims of a banking website could be redirected to a server managed by criminals who could use it to serve malware, or to induce bank customers to provide their credentials to a copy of a legitimate website. If an attacker spoofs an IP address; DNS entries for a bank website on a given DNS server, replacing them with the IP address of a server they control, makes an attacker able to hijack customers.

(10)Malware based-attacks

Malware based-attacks are one of the most among hazardous cyber threats related to electronic banking services. In such attacks a malicious code is designed. Now-a-days the number of malware attacks in banking sector has been increasing. Some of the infamous banking malware are Carbep, Tinba, Spyeye, Zeus and KINS. Zeus is the oldest out of these malware. It was detected in July 2007 when the information was lost and stolen from United States Department of Transportation. There are other malwares which have been identified in previous years to commit bank fraud on a large scale.[42] It has been noticed that almost every virus has two features, one, that they secure a backdoor entry into the system and they steal credential information of a user.

4. Recommendations To Prevent Cyber Crime

Banking sector is the backbone of our economy. The increasing number of cyber-crime cases has resulted in huge loses to our economy. Cyber-attacks should be prevented by ensuring suitable legislation which is implemented effectively. Both the banks and the customer should be made aware about the risk involved and safeguard measures. There needs to be cooperation between the various stakeholders to counter cyber-crime. The Indian Government established an Inter Departmental Information Security Task Force (ISTF) with the National Security Council as the nodal agency for the coordination of all matters relating

[42] http://articles.economictimes.indiatimes.com/20141105/news/55798224_1_malwarevirusbanking

to effective implementation of its cyber security strategy. Indian Computer Emergency Response Team (CERT-In) is the national nodal agency which is made to respond to computer security incidents whenever they occur. Few of the activities undertaken by CERT-In in implementing cyber security include coordination of responses to security incidents and other major events; issuance of advisories and time bound advice regarding imminent threats; product vulnerabilities analysis; conducting trainings on specialized topics of cyber security; and evolution of security guidelines on major technology platforms.[43]

One of the main issues related with cyber-crime is of jurisdiction. Cyber-crime can be committed in any part of the globe having its impact in any corner. Every citizen should be able to identify and report cybercrimes from anywhere regardless of the country they reside in. The existing systems present in India for reporting cyber related offences involves registering complaints with the local police stations or cybercrime cells. Many Indian states have setup cybercrime cells, which monitor such crimes. In several instances, where the victims of cybercrime may not be able to report a cybercrime due to several reasons, such as staying in a remote location, unawareness regarding the place to report and privacy related issues. This tends to result in many cybercrime cases going unreported. Since, there is no centralized online cybercrime reporting mechanism. Also for law enforcement agencies at various levels such as national, state, and local level, there is no centralized referral mechanism for complaints relating to cybercrime.[44] IT Act should be amended accordingly to define cybercrime and also specify the cases where the Act will have extra-territorial jurisdiction. The scope of the IT Act needs to be broadened to include legal framework relating to cyber laws in India. The responsibility of the intermediaries is vague and must be made more clear and explicit.

Some of the measures in which cyber-crimes can be prevented and reduced are:

4.1 Cyber Fraud Council in Banks

Whenever a cyber-fraud is committed the victim should report to the Cyber Fraud Council that must be set up by in each and every bank to review, monitor investigate and report about cyber-crime. In case, such Council does not take perform or refuses to perform its

[43] Strategic national measures to combat cyber-crime: Perspective and learnings for India, <http://www.ey.com/Publication/vwLUAssets/ey-strategic-national-measures-to-combat-cybercrime/$FILE/ey-strategic-national-measures-to-combat-cybercrime.pdf> August 2015.

[44] *Ibid*

duty then a provision to file an FIR must be made. The matter to be brought before such council can be of any value. However, when the value is high then the Council shall act expeditiously. RBI in its 2011 Report stated that when bank frauds are of less than one Crore then it may not be necessary to call for the attention of the Special Committee Board.[45]

4.2 Education to Customer

The customer should be educated and made aware about various bank frauds and measures should be informed to them for safety mechanisms so that they do not fall prey as victims of cyber-crime. If a customer is conscious and report the matter of cyber-crime then in the initial stage also instances of cyber-crimes can be reduced. A customer should be made aware about the Dos and Don'ts' of E-banking. It can be done through publishing it on the bank's website, publishing in the newspaper, through advertisements, by sending SMS alerts, through poster education etc. In case a bank introduce any new policy or there are any changes which are required to be followed by all banks as per RBI then, bank must inform the customer through mails or by informing the customer through telephone.[46] The awareness material should be timely updated keeping in mind the changes in the legislation and guidelines of RBI.[47]

4.3 Training of Bank Employees

Training and Orientation programs must be conducted for the employees by the banks. The employees must be made aware about fraud prevention measures. It can be done through newsletters or magazines throwing light on frauds related aspects of banks by senior functionaries, putting up 'Dos and Don'ts' in the workplace of the employees, safety tips being flashed on screen at the time of logging into Core Banking solution software, holding discussions on factors causing cybercrime and actions required to be undertaken in handling them. Employees who go beyond their call of duty to prevent cyber frauds if rewarded will also enhance the work dedication.[48]

4.4 Strong Encryption-Decryption Methods

[45] Reserve Bank of India, *Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds*, (21 Jan 2011)
[46] *Ibid*
[47] *Ibid*
[48] Supra note 161

E-banking activities must be dealt using Secure Sockets Layer (SSL). It provides encryption link of data between a web server and an internet browser. The link makes sure that the data remains confidential and secure. As per India, we follow asymmetric crypto system which requires two keys, public and private, for encryption and decryption of data.[49] For SSL connection a SSL Certificate is required which is granted by the appropriate authority under IT Act, 2000. To ensure security transactions RBI suggested for Public Key Infrastructure in Payment Systems such as RTGS, NEFT, Cheque Truncation System. According to RBI it would ensure a secure, safe and sound system of payment.[50] Wireless security solutions should also be incorporated. In cases of Denial of Service Attacks, banks should install and configure network security devices.

4.5 Physical and Personnel Security

Banks must execute proper physical and ecosystem controls giving regards to threats, and based on the institution's unique geographical location, and neighboring entities etc. Also when a new employee is employed then there should be a process of verification of the applicant. The level of verification may wary depending upon the position and job profile.[51] In ATMs there must always be a security guard who has received proper training under the force. It is because many incidents occur where ATMs are looted. So physical security at ATMs is necessary.

4.6 Cooperation among nations to avert cyber crime

Cyberspace being transnational in nature requires cooperation among States to work together to avert cyber-crime. Although, a few treaties and implementation measures exist; a wholesome approach defining legal and technical measures and organizational capabilities is yet to take central importance for India in its goal to contribute to the global fight against cybercrime. IT Act, 2000 having extra-territorial application poses a problem in investigation, prosecution and extradition of foreign nationals. India should actively engage

[49] Section 3(2), Information Technology Act, 2000 provides authentication of Electronic Records shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

[50] RBI for two stage verification for online banking transactions, *Economic Times*, Mumbai, April 22,2014

[51] RBI Guidelines on Information Security, Electronic Banking, Technology Risk management and Cyber Frauds, 2012.

as part of the international cybercrime community centered on Asia, Europe and America to seek help and also contribute to international cybercrime issues. [52]

5. Conclusion

The present conceptual framework has provided a bird's eye view of ongoing efforts to prevent and control highly technological and computer based crimes, and highlighting general trends and developments within and without the Indian banking sector. This study has described deeply a number of common electronic crimes, identified in the specific areas of Indian banking sector.

The study has provided an overview to the concept of E-banking by discussing deeply various cyber-crimes, identified specifically in the banking sector. The Banking system is the lifeblood and backbone of the economy. Information Technology has become the backbone of the banking system. It provides a tremendous support to the ever increasing challenges and banking requirements. Presently, banks cannot think of introducing financial product without the presence of Information Technology. However Information Technology has an adverse impact too on our banking sector where crimes like, phishing, hacking, forgery, cheating etc. are committed. There is a necessity to prevent cyber-crime by ensuring authentication, identification and verification techniques when a person enters into any kind of banking transaction in electronic medium. The growth in cyber-crime and complexity of its investigation procedure requires appropriate measures to be adopted. It is imperative to increase the cooperation between the stakeholders to tackle cyber-crime.

According to National Crime Records Bureau it was found that there has been a huge increase in the number of cyber-crimes in India in past three years. Electronic crime is a serious problem. In cases of cyber-crime, there is not only financial loss to the banks but the faith of the customer upon banks is also undermined.

Indian banking sector cannot avoid banking activities carried out through electronic medium as the study suggest that there has been an increase in the number of payments in e-banking. However, the change in the banking industry must be such which suits the Indian market.

[52] *Ibid*

Banks are required to be updated and ahead with the latest developments in the IT Act, 2000 and the rules, regulations, notifications and orders issued therein pertaining to bank transactions and emerging legal standards on digital signature, electronic signature, data protection, cheque truncation, electronic fund transfer etc. as part of overall operational risk management process.

It is the need of the hour to increase cooperation between the countries, over the tools and techniques, which will help them effectively, counter global electronic crime. In developing countries, like India, cyber and electronic crime poses a serious problem because there is a lack of training on the subjects related to investigation of electronic and cybercrimes.

Lastly, it can be concluded that to eliminate and eradicate cybercrime from the cyber space is not a seemingly possible task but it is possible to have a regular check on banking activities and transactions. The only propitious step is to create awareness among people about their rights and duties and to further making the implementation of the laws more firm and stringent to check crime.