International Journal of Management, IT & Engineering
Vol. 9 Issue 1, January 2019,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

ELECTRONIC FRAUD (CYBER FRAUD) RISK IN THE BANKING INDUSTRY, A STUDY WITH SPECIAL REFERENCE TO BIHAR.

*Dr.Kundan Kumar
Programme officer,Rural Development Department, Bodhagaya Gaya.
E-mail id kundan.kumard@gmail.com

Abstract
In the era of globalization Internet banking or online banking has revolutionized an integral activity of our modern twenty first century. The paper explores forms of electronic fraud which are being perpetrated in the banking industry and the challenges being faced in an attempt to combat the risk. The paper is based on a descriptive study which studied the cyber fraud phenomenon using content analysis. To obtain the data questionnaires and interviews were administered to the selected informants from 22 banks across Bihar. Convenience and judgmental sampling techniques were used. It was found out that most of the cited types of electronic fraud are perpetrated across the banking industry. Challenges like lack of resources (detection tools and technologies), inadequate cyber-crime laws and lack of knowledge through education and awareness were noted. It is recommended that the issue of cyber security should be addressed involving all the stakeholders so that technological systems are safeguarded from cyber-attacks.

Keywords: Electronic Fraud, Cyber Fraud, Cyber-Crime, Internet Banking, Electronic Banking

Introduction

In modern times banks are not so often robbed because money is not only kept in bank vaults. In modern computer technologies and data networks a lot of money exists in cyber space. Banks have to adapt to modern trends of doing business electronically and at the same time protect themselves against cyber-crimes. 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 BC in India, Japan and China. 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 cyber crime. The era of modern computers, however, began with the analytical engine of Charles Babbage. The first person to be found guilty

of cybercrime was Ian Murphy, also known as Captain Zap, and that happened in the year 1981. He had hacked the American telephone company to manipulate its internal clock, so that users could still make free calls at peak times. In Bihar almost all banks to date have implemented electronic banking and/or cyber banking in one way or the other.

Today computers have come a long way, with neural networks and nanocomputing promising to turn every atom in a glass of water into a computer capable of performing a Billion operations per second. With the increase in benefits of speedy and comfortable banking transactions internet and cyber frauds also proved sinister implications.

At the onset, let us satisfactorily define "cyber crime" and differentiate it from "conventional Crime". 166 Computer crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. Th e abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.In terms of banking frauds which 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 charging of the card owners.

History of banking frauds

On August 2, 2016, Bitfinex, a Hong Kong exchange for the trading of digital currencies, announced that some of its customer accounts were hacked and bitcoins stolen. The value of the stolen bitcoins has been reported to be approximately US$65 million or more. As a consequence the value of bitcoins came down and the trust on the digital currency shaken.

- In the beginning of the year 2016, Bangladesh Bank was the target and an attempt was made to steal US$1 billion and ultimately the attackers could successfully get away with US$81 million. Recently, in India too, a similar attempt was made on a commercial bank by generating fraudulent payment instructions on the Nostro accounts and transmitting them over SWIFT messaging system. Though monetary loss could be prevented with proactive follow-up with the concerned paying /

intermediary banks, the incident has reinforced the fact that the various stakeholders have not learnt the lessons yet. We have also come across instances of fraudulent messages confirming documentary credits being transmitted using SWIFT infrastructure. Although, the latter incidents were mainly a result of failure of internal controls and non-adherence to 'four eyes principles', it is also on account of reliance on disparate systems whereby SWIFT transactions could be done without originating a corresponding transaction in the CBS.

- In another incident involving shared mobile wallet of a bank, vulnerabilities were observed in the application itself which led to exploitation by the attackers. The originator of the transfer could get the amount reversed back to him without corresponding debit in the recipient's account in a large number of transactions (total amount involved was around □12 crore). Bank was not performing any real time reconciliation and noticed it only when there was a spike in transactions which led to detection during reconciliation. The vulnerabilities exploited in the incident could have been averted, had the launch of the product not been rushed through.

- In another incident, an e-payment validation website of a large bank was hacked. Surprisingly, the bank was not aware of the incident till it was notified by a law enforcement agency. There was a Facebook post by a person from a neighbouring country claiming responsibility for the operation. Though the hacking incident did not result in any pecuniary loss as the site attacked was only performing validations of inputs entered by end users, nevertheless it demonstrates a serious security breach.

As per National Crime Records Bureau-banking frauds in India , a total of 9,622 and 11,592 cases registered during 2014 and 2015, respectively.

In year 2016, the ICICI Bank topped the list of banks that had witnessed the most number of bank frauds, with state-owned SBI taking the second spot. In fact, in a matter of hardly 9 months, as many as 455 fraud cases involving sums of Rs. 1 lakh and above were detected in ICICI Bank, closely followed by SBI (429), Standard Chartered (244) and HDFC Bank (237).

Reserve Bank of India (RBI) has registered a total of 921 cases of fraud involving ATM/debit cards, credit cards and Internet banking, wherein the amount involved was Rs 1 lakh and above, during 2018-19.

As may be seen from the examples quoted above, the cyber threat landscape is widening. This is natural, given that the money no longer moves only in physical form, but mostly through electronic means. It opens avenues for unscrupulous elements to devise ingenious methods for stealing it. One of the key targets by the attackers is the credential of the customers, as it provides the key to the 'khazana (treasure)'. Recent experience shows involvement of organised gangs and nation-state actors having huge financial backing. On the other hand, the cost of orchestrating such attacks is coming down. There are several reports indicating availability of credentials of customers for sale in dark web, which is really scary.

Legal Regime to Control Banking Frauds in India

The Reserve Bank has recently issued on June 2, 2016 a comprehensive set of guidelines for Cyber Security framework in banks. These guidelines built over the earlier work emphasise the importance of having a focussed attention to cyber threats and framework for mitigating the threats and to protect the information assets.

The Reserve Bank of India has set up a 'working group on internet banking' to examine various aspects of the concept of net banking. The focus of these laws is on technology, legal, regulatory, supervisory, and security issues, and include the following aspects:

The Consumer Protection Act, 1986 defines the rights of consumers who are availing banking services. Since banking is a service that is defined in the Act, a consumer complaint can be filed against the bank for lack of safe banking services.

Section 3(2) of the Information Technology Act, 2000 provides for technologies to authenticate the source of electronic record. Banks are bound to comply with confidentiality of the customer's accounts. Banks in India have to provide a safety valve to the consumers.

Literature Review

BBC NEWS (27 March 2015) -Losses from online banking fraud rose by 48% in 2014 compared with 2013 as consumers increasingly conducted their financial affairs on the internet. The rise is due to increased use of computer malware and con-artists tricking consumers out of personal details. Overall losses on UK cards from fraud totaled £479m in 2014, up 6% on 2013, according to Financial Fraud Action. The total amount of fraud is down 21% from the peak of £609.9m in 2008. The figures also showed that losses caused by criminals using UK cards fraudulently abroad, where they can circumvent some security features, were up sharply. Losses increased to £150.3m in 2014,

up 23% from the previous year. The figures come in the same week as fraud prevention service Cifas said that 46-year-old men were the most likely victims of identity theft.

2. Business Standard (Mumbai July 10, 2015) With the increase in banking on mobile phones and the internet, financial frauds in the system have also seen an uptick, says a survey on financial frauds in the financial sector by Assocham and PwC. The report said that financial frauds led to approximately $20 billion (Rs 1.26 lakh crore) in direct losses annually. The report states that currently, 74 per cent of the population has mobile phones and this has led to a steady rise in banking on the go. According to Reserve Bank of India data, the volume of mobile banking transactions has risen from around Rs 1,819 crore in 2011–12 to approximately Rs 1,01,851 crore in 2014-15. Whether it's financial transactions, customer experience, marketing of new products or channel distribution, technology has become the biggest driver of change in the financial services sector. Most financial institutions are therefore insisting on cashless and paperless transactions.

3. Business Insider India (Jan 5, 2015) - consulting arm of Mahindra Group, suggests that the number of cyber crimes in the country is expected to double and cross the 3-lakh mark in 2015. As per the study, the cyber crimes are growing at a rate of 107% year on year while registering over 12,000 cases every month. According to the report, the number of cases of cyber crimes was 13,301 cases in the year 2011, which was followed by 22,060 such cases in 2012 and 71,780 cases in 2013. By May 2014 alone, the cyber cells in India had registered a whopping increase in cyber crime cases and registered 62,189 cases. The increasing use of mobile, smart phones, tablets for online banking and financial transactions has also increased the vulnerabilities to a great extent. The maximum offenders came from the 18-30 age groups, stated the report. The economic growth of any nation and its security whether internal or external and competiveness depends on how well is its Misuse of the ATM-cum-debit card had been a common problem for all. Often debit card users report fraudulent transactions have been made through their ATM cards even when the cards were in their possession.

4. Worldlypost(Karthik /January 5,2015)- Assocham-Mahindra SSG study has released a report stating the number of cyber crimes in India may double to 3 lakhs in 2015. India now being the favorite and easy to target for cybercriminals, mostly hackers, other malicious users could pose serious economic and national security challenges. India has been prone for all the identity theft, spamming, phishing and other types of fraud, as there is an upturn usage of Smart phones and

tablets for online banking and other financial transactions in recent times. The Study also revealed that ―the US, Europe, Brazil, Turkey, China, Pakistan, Bangladesh, Algeria and the UAE‖ are the countries from where most of the cyber space attacks have been originated, which is a major concern. India ranks third after Japan and US in the list of countries most affected by online banking malware during 2014. As per the study, Andhra Pradesh, Karnataka and Maharashtra are in top three positions in 2014 when it comes to the number of cyber crimes cases registered under the new IT Act in India. It further added, these three states together contribute more than 70 percent to India`s revenue from IT and IT related industries

5. **PTI New Delhi (January 5, 2015 7:04 pm**): The increasing use of smart phones and tablets for online banking and other financial transactions have increased risks. Rising at an alarming rate, the number of cyber crimes in the country may double to 3 lakh in 2015 and could pose serious economic and national security challenges. India has emerged as a favorite among cybercriminals, mostly hackers and other malicious users who use the Internet to commit crimes such as identity theft, spamming, phishing and other types of fraud. As per the study's findings, total number of cyber crimes registered during 2011, 2012, 2013 and 2014 stood at 13,301, 22,060, 71,780 and 1, 49,254 respectively. The origin of these crimes is widely based abroad in countries like China, Pakistan, Bangladesh and Algeria, among others. Phishing attacks of online banking accounts or cloning of ATM/debit cards are common occurrences. Maximum number of offenders belong to the 18-30 age group, added the report. The study revealed that the attacks have mostly originated from the cyber space of countries including the US, Europe, Brazil, Turkey, China, Pakistan, Bangladesh, Algeria and the UAE. It further stated that mobile frauds are an area of concern for companies as 35-40 per cent of financial transactions are done via mobile devices and this number is expected to grow to 55-60 per cent by 2015.Rising Internet penetration and online banking have made India a favorite among cybercriminals, who target online financial transactions using malicious software (malware). India ranks third after Japan and US in the list of countries most affected by online banking malware during 2014, the study said. Andhra Pradesh, Karnataka and Maharashtra have seen the highest number of cyber crimes registered under the new IT Act in India. Interestingly, these three states together contribute more than 70 per cent to India's revenue from IT and IT related industries

International Journal of Management, IT & Engineering
Vol. 9 Issue 1, January 2019,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Objective of study

To ascertain the current scenario of cyber crimes in India the following are objectives.

1. To analyze the categories of cyber crimes in banking sector.
2. To review the tricks/ techniques used by cyber criminals.
3. To review the current scenario of cyber crimes.
4. To provide set of instructions to be followed as a victim of cyber crime.
5. To suggest the preventive measures and safety tips to control and prevention of cyber crimes.

Methodology Used

This study is based on secondary data. To fulfill the first objective of the study the category of cyber crimes is analyzed by reviewing various literatures and Information Technology Act 2000 as well as the web site of cyber crime investigation cell Bihar. To review the tricks and techniques used by cyber criminals to hack the banking systems and make the cyber frauds various case studies in various news channels are referred. To review the status of cyber crimes in India and Bihar the data is gathered from annual reports of National Crime Record Bureau (NCRB).

Various Cyber attacks in banking sector

The most common types of online fraud are called phishing and spoofing. Phishing is the process of collecting your personal information through e-mails or websites claiming to be legitimate. This information can include usernames, passwords, credit card numbers, social security numbers, etc. Often times the e-mails directs you to a website where you can update your personal information. Because these sites often look "official," they hope you'll be tricked into disclosing valuable information that you normally would not reveal. This often times, results in identity theft and financial loss.

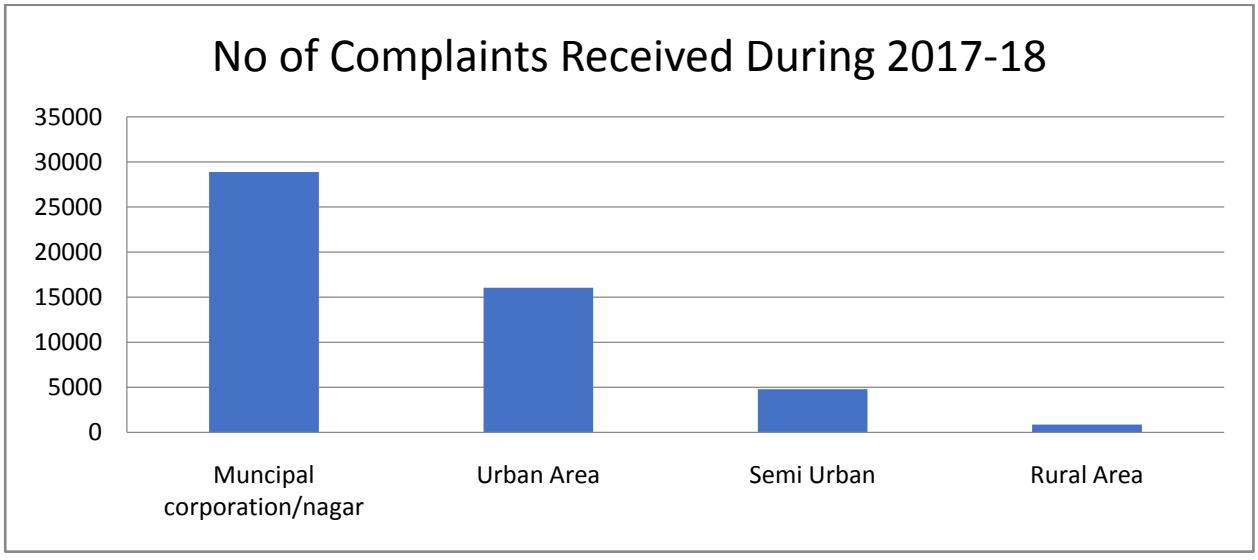
Spyware and viruses are both malicious programs that are loaded onto your computer without your knowledge. The purpose of these programs may be to capture or destroy information, to ruin computer performance or to overload you with advertising. Viruses can spread by infecting computers and then replicating. Spyware disguises itself as a legitimate application and embeds itself into your computer where it then monitors your activity and collects information.

International Journal of Management, IT & Engineering
Vol. 9 Issue 1, January 2019,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Fraudulent "Pop-up Windows" are a type of online fraud often used to obtain personal information. They are the windows or ads that appear suddenly over or under the window you are currently viewing. Fraudulent websites or pop-up windows are used to collect your personal information. Other terms for the fraudulent process of gathering your personal information include "Phishing or "Spoofing." Additional links to real websites can be incorporated into the email to lead you to believe the email is legitimate.

Current Scenario of Cyber Crimes Related Banking Sector in Bihar

Bank group-wise classification

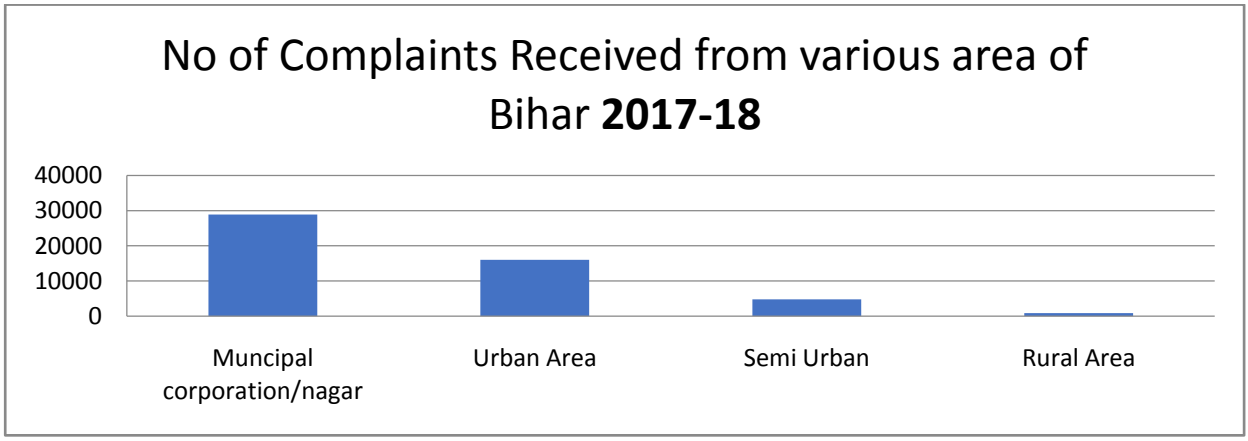


(Source: Annual Crime Report of RBI 2017-18)

The above graph shows the bank group wise classification of complaints received during 2017-118. It is seen that more complaints are received from Nationalized Banks group (24391) which follows SBI & Associates(24367), Private Sector Banks(17030), Foreign Banks(5016) and Others(4179). Very less complaint are received from RRBs/ Scheduled Primary Urban Co-op. Banks (1590)

International Journal of Management, IT & Engineering
Vol. 9 Issue 1, January 2019,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Bank Area-wise classification



(Source: Annual Crime Report of RBI 2017-18)

In the above Graph we can see urban area more prone to cyber crimes may be one of the reason that in rural or less developed area people use e-banking.

Conclusion

To review and analyze the current scenario of cybercrimes, we focused on the annual reports of National Crime Record Bureau (NCRB), Indian Computer Emergency Response Team (CERT), Internet Crime Complaint Center (IC3) ,the Global Information Security Survey 2014-15, Press Information Bureau English Releases, Reserve Bank of India publications. The findings of this research paper shows that the IT usage and cybercrime related to online banking in India are on the rise. Majority of the cybercrimes have been committed by young people in the age group 18-30and are male gender. Our law enforcement agencies need to be adequately equipped to overcome and prevent the cyber crime. In e-banking, the core security areas must be paid utmost attention-confidentiality, integrity and availability. Banks are required to restructure, reinvent and reengineer themselves to meet the necessary criteria, offer better products and acquire the competitive edge. The shift in the banks from traditional to modern e-banking services has been welcomed due to its advantages but Indian banks are taking time to get rooted. If e-banking is handles in the right manner by banks and customers, then it would take the economy to great heights.

References

- Cyber crime News:http://www.computerweekly.com/news/2240215532.Financial-services-sector-attract-mostcyber-crime.
- Dr.Satyadevi,C (2009)-"Financial Services-Banking and Insurance", pg 77-83
- Dr. Miryala,Ramesh Kumar and Reddy,M.Venkat Ramana (2015)- trends, challenges and Innovations in Management.
- History of Banking: http://en.wikipedia.org.wiki/Banking_in_India
- Mithani,D.M.; Gordon,e. (2007)-"Banking and financial Systems", pg 121-140
- Pradhan,Rudra Prakash (2009)- "Forecasting Financial Markets in India", p 76-85
- Tripathy, Nalini Prava (2007) "Financial services", pg 201
- Sharma, K.C. (2007) - "Modern Banking in India", page 239
- R. Gandhi - Targeted Attacks: Protection of Critical Infrastructure of the Country & Capacity Building –
- S. S. Mundra 2016-Information Technology & Cyber Risk in Banking Sector – The Emerging Fault lines.
- Susheel Chandra Bhatt and Durgesh Pant(2011): Study of Indian Banks Websites for Cyber Crime Safety Mechanism,(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.10, Jayshree Chavan(June 2013): Internet Banking- benefits and challenges In An Emerging Economy, International Journal of Research in Business Management (IJRBM) ,Vol. 1, Issue 1, 19-26.