Inspira-Journal of Commerce, Economics & Computer Science (JCECS)
ISSN : 2395-7069 COSMOS Impact Factor: 4.964, Volume 06, No. 01, January-March, 2020, pp. 21-27

CYBER CRIME AND CYBER SECURITY IN INDIAN BANKING SECTOR

Dr. C.Mallesha*

ABSTRACT

In today's world, India has seen a huge increase in Cyber crimes such as Trojan attacks, e-mail bombing, information theft, system hacking, data hacking etc. Despite various technologies are used by organizations, there is rise in cybercrimes in the recent years. Since computer usage and internet usage have been increasing rapidly in day to day life there is a large scope of cyber crime that can be done by fraudsters. In this concern there should be some precaution measures to be done when individuals and corporates offices are using internet as it is major threat in cybercrime. The purpose of the study is to represent the various types of cybercrime in banking sector and their effect on the banks. In this paper certain preventive measures have been suggested to reduce the cyber crime and basic cyber security points are discussed.

KEYWORDS: *Cyber Fraud, IT Act, Indian Banking Sector, Cyber Security, Cyber Law.*

Introduction

As the Information and Computer Technology has made its reach into almost in every one's life. The world has seen a growing trend of using online transactions, digital data transfer, electronic database and so many business, social and other activities based on computers, internet and information technology tools. Banking, insurance and financial organizations are the prime users of internet and online transactions. They make use of such technology to transfer cash, make payments, submit account information and other kinds of remittance services. Owing to these services in banking sector has increased a lot with usage of internet but threat regarding the cybercrime is a major threat. Both the data and transactions related to online are attacked. Online transactions and data are not free from being attacked or manipulated.

Cybercrimes include hacking of information regarding the accounts, the data is hacked in the systems, debit and credit cards scams, scams in ATM etc., are considered majorly as the scope for thefts in banking system. In the recent year's utilization of online as a source for banking transactions has been tremendously increased and this way a chance for cyber criminals has also been increased with heavy loss in the money.

Cyber Crime Definition

Cyber crime is a digital wrong doing. Any illegal activities committed using a computer or by using the net is known as cyber crime. It includes both monetary and non-monetary thefts. Non-monetary thefts are those in which data regarding the account, details such as debit cards credit cards, viruses in the computer or hacking most confidential information from the banking system. Whereas monetary includes from ATM theft to million rupees from the banking system. This deliberate act committed by any individual is booked against cyber criminals. To reduce or to overcome this risks banks should adequately step by taking repetitive audits both internal and external audit.

---

* Assistant Professor, School of Business Management, Anurag Group of Institutions, (An Autonomous Institution), Venkatapur (Village), Ghatkesar (Mandal), Medchal, Telangana State, India.

Cyber crime is a crime that is committed online in many areas using network and e-commerce. A computer is used for an offense when an unapproved access of computer system happens and on the other hand it influences ecommerce. Cybercrimes are of different types, for example, Funds transfer fraud, money laundering, investment fraud, sales fraud etc. The present contemporary period has replaced the customary fiscal dimensions right from paper money to plastic cash as a Master card, credit card, debit card etc. This has brought about the expanding utilization of ATM everywhere throughout the world. The utilization of ATM is safe as well as advantageous and also convenient. In the front side plastic cash such as Debit cards and credit cards as convenient but slight misuse of the cards is the major threat. This is regarded as ATM fraud which is the major burning issue. Information and Communication Technology (ICT) has made our everyday lives simpler in different aspects at each stage but at the same time there have been consequences in arising different form of crimes. The businesses process has been simpler because of technologies innovation.

Law as the regulator of human behavior has made an entry into the cyberspace and is trying to cope with its manifold challenges. Certain acts such as E-Commerce Act, 1998 came into force as a legal frame work onto the cyber world in India to enact on the cybercrimes. Then emerging of the Information Technology Act, 2000 in force for the cyberspace transactions and this was updated with few modifications by the committee in 2008. This IT act amends few of present existing laws such as Reserve Bank of India Act, Indian penal code Act, Indian Evidence act etc. Although there is an introduction of acts implementation of these acts is still on papers but in practical their execution is not to complete stage because understanding the terminology is major issue for lawyers, police, and other officials. Few important cyber crimes include hacking, fraud, pornography, cyber terrorism etc.

Introduction to Cybercrime in Banking Sector

The first ever email spam has taken place in the year 1976 whereas first cybercrime has taken place in 1820. In the year 1982 first virus was installed in apple computer. Till mid 90's the banking system was simple and reliable however there has been a shift in the banking sector with technological interventions. Banking sector has introduced many technological platforms for customers to make the work easier and for in time completion, with this there is are 24*7 and throughout the year access to process the requests of the customers. For example, ATM and online banking procedures are processed continuously. However, with the enhancement of banking technology, there a rise in frauds also.

Both the information and money in the banks are stolen by the cybercriminals using different means. In a study conducted by Anderson et al (2012) focused on that banks have lost billion dollars due to the frauds and this various details regarding the cybercrimes the are committed all over the globe and they are both direct and indirect losses. In order to reduce and protect from the frauds both the banks and regulatory bodies have to make and frame the policies and regulations. There are control measures taken to have a glance on the transactions related frauds, but still the frauds are not mitigated. The main reason behind this is the present using techniques and the measures are time taking and are available in public domain by this even the cybercriminal can access the adopted measures to overcome the defenses. The cybercriminals find different solutions to overcome these measures.

To mitigate and reduce the cybercrimes in banking system one of the ways is to detect the factors that are main targets of cyber-attacks. A study by Moore and Clayton (2007) mostly all the banks are frequently targeted for the crimes and the malware attacks such as phishing, identity theft etc. The study also described why most banks are targeted for the malwares which includes the market size, money transfer policies and also in which location the banks are located can be one of the pre requisites for the cyber criminals. According to Sherstobitoff, 2013 some of the banks are more specific to the malware attacks.

Literature Review

A review of the work done in the area of Electronic crime or Cyber crime or Computer crime. In this paper some of the pertinent literature available scanned which are collected from various research papers, articles and books related with the topic which shows that work have been conducted out in the area of Electronic crime by several researchers They are:

Gupta P.K. in his study entitled 'Internet Banking in India – Consumer Concerns and Bank Strategies' studied about the conventional banking limitations and to know the patterns of customer awareness levels, their satisfaction and importance and knowledge of the Internet banking. The study also described about the various strategies in banking system for the adoption of internet and also the study includes the regulations of the internet banking.

Ashu Khanna, Bindu Arora conducted a study with the title 'A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian banking industry'. In this study various measures that are taken by the employees and the management of the bank to reduce the cyber crimes are observed. The awareness and the knowledge regarding the frauds and the measures are not up to the mark in case of employees as they lacked in understanding the terminology related to the auditing and they faced difficulty in following the guidelines given by RBI because of the work pressure in the present competition.

Hemraj Saini, T.C. Panda and Yerra Shankar Rao with title 'Cyber-Crimes and their Impacts: A Review' have studied about different types of cyber crimes and the effects of these cyber crimes in different segments in the society in general.

Singh in his study on 'Online Banking Frauds in India' mentioned the cybercrimes in India with rise in information technology. As there are very less cyber law firms in India and the cyber crimes are not properly reported. The cyber security in developing countries is still in increasing stage.

Moore.T, Clayton.R & Anderson.R (2009) described on the cybercrimes and hackers are creating a major problem in the present banking industries. The study also focused on significant improvements are possible in the way dealing with online fraud and to study the online crime it is suggested that to understand its economic perspective.

Muthukumaran.B (2008) in his article focused on the term cybercrime and its emerging practices in India. This article is based on several survey report, news, media and news portals to gave a wide synopsis of the cyber crime emerging practices such as cyber stalking, hacking, phishing, cyber squatting, vulnerability etc. this article is an effort to checkmate the undesirable fall out of youngsters assessing the internet and at higher rate..

According to Business Standard magazine there is a sharp rise in usage of internet for banking services as well as there has been an increase in financial frauds based on the survey conducted by ASSOCHAM and PwC. There has been a huge loss incurred due this financial fraud which counts to approximately Rs.1.26 lakh crore. Almost 74 % of the population has been using mobile phones for banking services. All the financial institutions have initiated cashless paperless transactions in banking services.

PTI New Delhi (January 5, 2015 7:04 pm): Increasing the financial transactions through online by smart phones and tablets also increased he risks of financial frauds. At the alarming rate there has been double in the number of frauds in the year 2015 and there is a great challenge for economic and national security. Identity theft, phishing, spamming and other types of fraud most happening in India.

Objectives of the Study

- To study the categories of cyber crimes in banking sector.
- To review about the cyber security in banking.
- To suggest the preventive measures for prevention of cyber crimes.
- To suggest certain safety tips.

Cybercrime in Banking Sector

Douglas and Loader (2000) defined cybercrime as computer mediated activities by electronic networks globally which illegally performed by certain parties. Cyber crimes in banking sector are committed through online technologies in illegal transfer of money and data

Four different types of cybercrimes are categorized according to Wall (2001). They are; cyber-violence, cyber-deceptions, cyber-pornography, cyber-trespass. Money laundering, credit card fraud, ATM frauds etc. are observed in banks. Over all the goal of the frauds and crimes is to get funds present in the banks through various modes.

Banking sector provides many facilities to their clients and internet banking, credit card, debit card, online transfer facilities are to customers and the customers can utilize these facilities 24 hours from any pace of the world with help of internet. As we all known that as these facilities are beneficial for the customer but it also has an evil side in which hackers and thefts are included. They make the misuse of such facilities and by hacking banking sites and customers account make a mess up in accounts.

Types of Cybercrime in Banking Sector

- **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, 2000.2 But under Section 43(a) read with section 66 of Information Technology (Amendment) Act, 2008 and Section 379 & 406 of Indian Penal Code, 1860 a person or a hacker can be punished. If such crime is proved then for such hacking offence the accuse 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 also a bail able offence.

- **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 evil3. If electronic transactions are not secured the credit card numbers can be stolen by the hackers who can misuse this card by impersonating the credit card owner.

- **Email Fraud**

In present period of life e-mail and websites are become a speedy, easy and preferred means of communication. some times by email fraud is made some of the hacker or a evil organization send email to bank customers that “congratulation you have won such a huge amount to enchase it please share your bank details” and by such customer simply have to type credit card number into www page off the vendor for online transaction or for enchase of such kind of amount then hacker make a miss use of such detail and make a crime which is also known as cyber crime as per law.

- **Phishing**

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication 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, secret word 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 institution’s 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. 4 F-Secure Corporation’s outline of ’information security’ dangers amid the first 50% of 2007 has uncovered that the study discovered the banking industry as vulnerable objective for phishing tricks in India.

- **Vishing**

Vishing is the criminal practice of using social engineering and voice over IP to gain access to private persona and financial information from the public for the purpose of financial reward. The term is a combination of voice and phishing. Vishing exploits the public’s trust in landline telephone services. Vishing is typically used to steal credit card numbers or other information used in indentifies theft schemes from individuals.

- **Cyber Stalking**

Cyber Stalking is use of the internet or other electronic means to stalk someone. This term is used interchangeably with online harassment and online abuse. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly such as flowing a person, appearing at a person’s home or place of business, making harassing phone calls, or vandalizing a person’s property.

- **Cyber Security In India**

Cyber security standards are security standards which enable organizations to practice safe security techniques to minimize the number of successful cyber security attacks. Cyber security refers to the technologies and processes designed to protect computers, network and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals. Cyber Security involves protection of sensitive personal and business information through prevention, detection and response to different online attacks. Cyber security actually preventing the attacks, cyber security. Privacy policy: Before submitting your name, e-mail, address, on a website look for the sites privacy policy keep software up to date: If the seller reduces patches for the software operating system your device, install them as soon as possible. Installing them will prevent attackers which will be difficult for thieves to guess. Do not choose option that allows your computer to remember your passwords. Disable remote connectivity: some PDA'S and phones are equipped with wireless technologies, such as Bluetooth, that can be used to connect to other devices or computers. You should disable these features when they are not in use.

Advantages of Cyber Security

- Critical attacks can be identified and defended by cyber security.
- Browsing of website can be done.
- Both the incoming and outgoing data in the computer can be processed.
- It will alarm from hacks and virus.
- Cyber security in PC needs to ne update in frequent intervals.

Safety Tips to Cyber Crime

- Checking settings.
- Backup to be maintained.
- Use the secure settings.
- Delete an uninstall all the unnecessary software's and documents.
- Antivirus software to be installed.
- Firewalls and pop blocker to be inserted.
- Strong passwords to be used and need to change them at regular intervals.

Preventive Measures to Control Cyber Crimes in Banking Sector:

Challenges: Fighting and preventing cyber criminals from damaging infrastructure is very serious challenge to our law and enforcement agencies. It is often difficult to determine the cyber criminal and their community. The techniques used by cyber criminals are continuously evolving and making it more challenging.

The following are some challenges of cyber crimes related to mobile and online banking:

- **Tracking the Origin of Crime:** Tracing cyber criminals are very difficult because criminal investigations and criminal activity itself is borderless by nature.
- **Growth of the Underground Cyber Crime Economy:** The fight against cyber crime is the growth of an underground cyber crime economy. The underground economy attracts many digital experts and talented individuals with a specialty around cyber initiative.
- **Shortage of Skilled Cyber Crime Fighters:** skilled manpower is requiring implementing cyber security measures and encountering such cyber attacks.
- **Widespread Use of Pirated Software:** the most important challenge is preventing the cyber crime. The prevalence of software piracy, as pirated software is more prone to attacks by viruses, malware and Trojans.

Safety Tips and preventive measures for Online Secure Transaction:

- Frequently check the online account and all the transactions whether the network is properly secured or not. Avoid online shopping and banking if network is not secure.
- Don't click on the link which are given in a spam email. They are considered as phishing from fraudsters.

- Check regularly and delete all the spam emails and empty the trash box to avoid clicking the mail accidentally.
- Ensure that mail you received is safe and secure emails such as lotteries messages, calls and emails are not safe and please don't respond for these types of calls, emails.
- Check whether the website using for online transactions is secure or not. Please don't provide CVV number to anyone.
- Immediately inform to the bank or credit card issuer when it is misused or lost.
- Don't share the bank credential details in public or in phone.

Suggestions of the Study

It is always necessary to take some preventive measures to prevent banking transactions from banking frauds and other threats. For this, the following suggestions can be made:

- Make sure with a protection program that gives power over cookies that forward information back to Web sites.
- Make sure web servers in a row public site are physically separate and individually confined from in-house corporate network.
- Bring into play latest anti-virus software, operating systems, Web browsers and email programs
- Place firewall and develop your content off line.
- Forward credit card information just to safe and sound web sites
- If Web site serves up active content from a database, consider putting that database behind a second interface on your firewall, with tighter access rules than the interface to your server.
- Systematically confirm out the site to business regularly.
- Don not forgets to verify out the site you are doing business carefully
- Don't transmit credit card information to unfamiliar sites
- Don't reveal password with other people

Conclusion

In India the cybercrimes are rising significantly. The offences such as social media, credit card fraud, phishing, and virus, Malware, Denial of services, Gambling, Hacking, Personal data breach, corporate data breach and virtual currency are repeatedly done by cyber criminals. The present conceptual framework has provided a brief overview of computer related crime, and number of common electronic crimes, identified in the specific areas of Indian banking sector. The internet is the medium for huge information and medium of communication around the world, it is necessary to take certain precautions while operating it. To prevent the cybercrimes, it is necessary to take certain precautions while operating the computer or internet. It is very important to educate every one and make them aware of cyber crimes and punishments –penalties for safe surfing and browsing, make them aware how to use and handle mobile and online banking, how to secure personal information, how to use various applications, what precautions has to be taken while doing online banking transactions. It is necessary to strong enforcement of cyber crimes rules and regulations. In developing countries, like India, electronic crime is a serious problem because there is a lack of training on the subjects to investigate the electronic crime. The ATM fraud is not the sole problem of banks alone. It is a big threat and it requires a coordinated and cooperative action on the part of the bank, customers and the law enforcement machinery.

References

~ Assocham India: Cyber crimes in India, study by 2015,The Associated Chambers of Commerce & Industry of India

~ BS Reporter (Mumbai July 10, 2015 Last Updated at 00:41 IST)- Cyber frauds on rise with increase in digital banking: Assocham -PwC, Business Standard, retrieved from: http://www.business-standard.com/article/finance/cyber-frauds-on-rise-with-increase-in-digital-banking-assocham-pwc-115070901104_1.html.

~ Computer Emergency Response Team(CERT):http://cert.India.com

~ Cyber Crime complaints 2015:http://rbi.org.in/Press-release

~ Cyber crime News: http://timesofindia.indiatimes.com/tech/tech-news/cybercrimes-up-across-India-Maharashtra-tops.

~ Cyber Crime News:http://ibnlive.in.com/news/cyber-crimes-up-by-51-percent-india-Maharashtra-ap-Karnataka-top-list.

~ Cyber crime News:http://www.computerweekly.com/news/2240215532.Financial-services-sector-attract-most-cyber-crime.

~ Cyber Crime: A Financial Sector View, Government and Public Sector, NASSCOM.

~ Gupta P.K., Internet Banking in India–Consumer Concerns and Bank Strategies, Global Journal of Business Research, 2(1), (2008)

~ History of Banking: http://en.wikipedia.org.wiki/Banking_in_India.

~ Karthik (January 5,2015),Cyber crime to Double in India by 2015: A Report , world post

~ Kevin Peachey (27 March 2015) Online banking fraud 'up by 48%', BBC NEWS , Personal finance reporter From the section Business retrieved from: http://www.bbc.com/news/business-32083781.

~ Khanna Ashu and Arora Bindu, A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian banking industry, Int.J.Bus. Sci. & App. Mgmt., 4(3), (2009)

~ Moore.T, Clayton.R & Anderson.R (2009). "The Economics of Online Crime" , Journal of Economic Perspectives, Volume 23, Issue no.3, Summer 2009, pp.3-20

~ Muthukumaran.B (2008). "Cyber Crime Scenario in India" , Criminal Investigation Department Review, January, pp.17-23.

~ National Crime Record Bureau: Cyber Crime Statistics In India 2014: http://ncrb.gov.in/pdf

~ PTI New Delhi (January 5, 2015 7:04 pm): Cyber crimes in India likely to double Published, retrieved from URL-http://indianexpress.com/article/technology/technology-others/cyber-crimes-in-india-likely-to-double-in-2015.

~ Purba Das (Jan 5,2015,03.48 PM)- cyber crimes to surge in India Likely to Touch 3 Lakh, Business Insider, Retrieved from:http://businessinsider.in/cyber-crimes-to-surge-in-India-Likely-to-touch.

~ Rupinder Pal Kaur(Aug.2013)-Statistics of Cyber Crimes in India: An Overview, International Journal of Engineering and Computer Science ,Vol 2,Issue 8.

~ Saini Hemraj, Rao Yerra Shankar and Panda T.C., Cyber-rimes and their Impacts: A Review', IJERA, 2(2), 202-209 (2012)

❑❑❑