Law Journals
A Treasure Trove of Legal Knowledge.

National Journal of Cyber Security Law
Volume 1, Issue 2
www.stmjournals.com

Flaws in E-Banking: A Prey to Cyber Hunters

R.B.Rishabh[1,*], B. Yamuna Saraswathy[2]
Student, School of Excellence in Law, Tamil Nadu Dr. Ambedkar Law University, Chennai, Tamil Nadu, India

Abstract

The term e-banking is a contemporary term, which derives its origin from the recent past. Banking products and services are provided by e-banking through information technology (IT). The ever-growing IT has led to the speeding up of banking transactions, increasing effective communication between the bank and its customers. To add on, the cut-throat competition has pushed the banks to adopt e-banking concept. Though the e-banking system has got couple of merits, it is not free from security threats. To be particular, the online banking accounts are mostly falling as a prey to cyber hunters. These cyber hunters are instigated as the e-banking products and services have opened a gateway to millions of people's information. This ultimately results in the infringement of privacy of customers by cyber hunters. On the same note, there is a need to implement stringent cyber-security measures to protect the privacy of the customers. This article aims to cast light upon the concept of electronic banking and various security threats in e-banking sector. The paper also analyzes how these security threats infringe the privacy of the customers. Further, the paper statistically analyzes the recent e-banking breaches. The authors give an insight about the regulatory and legal framework with regard to e-banking crimes and provide suggestions for betterment of such laws.

Keywords*: Cyber-crime, Cyber security, E-banking, Information technology, Privacy*

****Author for Correspondence*** E-mail: rbrish97@gmail.com

INTRODUCTION

Electronic banking (e-banking), a relatively new term to the Indian society, owes its credit to liberalization, privatization, and globalization (LPG) movement which has freed the society from the clutches of regulations of the government to be a de-regulated economy. In the current scenario, the impact of information technology (IT) is crucial in any service-oriented industry and the banking industry stands no exception to it. Gaining access to IT is to be regarded as a major contribution to the growth of e-banking field. Today, all major banks provide e-banking facilities to their customers. E-banking services have reduced cost and workload to its customers and branches respectively. At present all major banks provide e-banking services, which have brought in cut-throat competition in this industry. Though the fruits of information technology taste good, the rapid developments in the technological perspective of the banks have to cope with the high compliance costs. E-banking is gaining pace in developed as well as developing countries. The products of e-banking technologies such as Automated Teller Machines (ATMs), internet banking, mobile banking, etc., prove to be a revolution in the contemporary banking system. Through e-banking the customer will have all details of his/her accounts on his palm. E-banking has contributed to the safeguard of the environment as well by going paperless. Nowadays, people relay on information provided by digital applications over to the information rend from the people which proves to be an emerging sign for services through information technology. Although the e-banking services have reduced the number of visits, which each customer makes to their banks, the physical branches of the bank cannot be completely replaced by e-banking products because the very customer expects a personal touch while availing banking services. Banks have moved on to the Core Banking Solutions (CBS) and back office of the banks has been shifted from the branches to a centralized zone. The e-banking products have been designed to function to run 24/7,

which really tests the ultimate potential of IT. The advent of information communication technology (ICT) has opened the cyber space so that it could be infringed by cyber criminals. The more and more the systems are breached, more and more personal data information (PDI) is acquired by the cyber hunters. We can therefore come to a conclusion that privacy of the internet users is at stake. In recent years the number of cyber crimes has drastically gone up. E-banking activity is being regarded as a lucrative prey for criminal activities and now the cyber criminals have been practicing unimaginable sophisticated techniques to hunt the e-banking sites or applications. The main reason why cyber criminals consider e-banking as a lucrative prey is because of the increasing number of users who are accessing these sites and applications. The main concern relating to the insecurity in e-banking service is that this sector lacks the awareness from the regulatory authorities. The government has to either make the available laws pertaining to security of e-banking stringent or come up with an exclusive law so as to ensure the security of e-banking products and services. The basic idea behind the cyber hunters is to procure the personal data information in order to commit cyber-crimes pertaining to data such as identity theft, cyber stalking, site cloning, etc. They do not just indulge in data-related crimes but also commit cyber terrorism through software-related means such as Trojan, spyware, hacking, phishing, smishing, vishing, spamming, spoofing, salami attack, money laundering, etc. Whatever it be, the trend of people availing e-banking services has not come down amidst the cyber hunters.

EVOLUTION OF E-BANKING

E-banking is the process of using the internet to organize, examine, and make changes to bank accounts, investments, etc. [1]. The term e-banking was first coined in 1980s and it became popular only in the mid-1990s. During its foundation years, usage of e-banking was through a telephone line. It was first in the US where the banking services in an online mode were used using the video tech system. In UK, a system known as Prestel System which had used a computer linked to a telephone line and a television set. Earlier, online banking was provided with an option for only a couple of services such as payment of gas, electricity, and phone bills.

The success of e-banking depends upon a customer's adoption of it. At the beginning, even setting up of a webpage to provide details or information regarding the products and services of the bank was considered as internet banking. Presently at an advanced level, it provides various facilities such as transfer of funds, buying of shares and insurance, accessing different accounts, etc. The most exciting advantage of internet banking is that all the services can be availed in the blink of an eye. Through e-banking one could pay taxes, book railways and air tickets, buy products online, apply for loans, etc.

Thulani [2] has identified three functional levels of internet banking which are informational, communicative, and transactional. Under informational level, the banks have provided marketing information on a standalone server regarding bank's products and services. Here in this case, the risk under information system is very low since there is no established link between bank's internal network and the server. Under the communicative level of internet banking there exists interaction between the customer and the bank's system. The last but not the least is the transactional level of internet banking which facilitates a customer of a bank to transfer funds from one account to other person's account, pay bills, etc. In this level of internet banking, the risk involved is pretty high compared to the other two levels of internet banking. Therefore, security measures at the transactional level of internet banking have to be tightened so as to safeguard the information of such accounts of customers from the cyber hunters.

E-BANKING RISKS

As we all know, the rapid growth of e-banking owes its credit to people's acceptance as well as to its cost-efficient mechanism. Like human behavior which has two extremes a positive and a negative one, the e-banking has proved to be a cost-efficient mechanism on one hand and on the other hand it has exposed itself to a variety of risks. A point which is to be noted is

that technology acts as both a source of risks as well as a medium to effectively control such risks. The following are various types of risks occurring in e-banking.

1. **Operational Risk**
   Operational risk is also known as transactional risk. It not only occurs due to inefficient technology, but also due to human negligence. Forms of operational risks are inaccurate processing of transactions, unauthorized access, fraudulent activities by employees and hackers, etc. The main reason for operational risk is inefficiency in design and lack of efficient monitoring of bank's information system.
2. **Reputational Risk**
   For a banking company to be successful in its industry, it is necessary to gather the support of its customers. So reputation plays a major role in determining the success of a banking company. A bank's reputation will be at stake when they receive a negative opinion from the public which does result in loss of funding and as well as loss of its customers. It also impairs public confidence and it also puts the banker and customer relationship at stake. The main reasons for this risk could be the defective systems prevalent in the bank, a malware or a virus in the banking system, or any other insecurity prevalent in the bank. At times, some disruption could lead not only a single bank reputation at stake but would create a wave throughout the banking industry arena.
3. **Money Laundering Risk**
   The main root cause of money laundering risk is that there are no proper KYC norms to spot in report the various unscrupulous activities in e-banking transactions.
4. **Cross-Border Risk**
   The ultimate aim of e-banking services is to reach customers at various geographical boundaries and this at times causes various risks. These risks occur because the loss of one country differs from that of another. Thus the risks are non-compliance of various countries' national laws, regulations, privacy rules, record keeping requirements, etc. It also paves way to credit risks when customer applies loan from a different region because he is from an unfamiliar customer base. The banks even while accepting foreign currencies at times during e-payments are under a risk that the foreign currency could largely fluctuate on the basis of exchange rate.
5. **Security Risk**
   Though the security risks were prevalent in the past, with the advent of e-banking, leaking information has drastically gone up. Back then banks functioned in a secluded environment whereas now banks function in an open environment which exposes them to security risks. Majorly the security breaches are committed due to criminal motive, casual hacking and due to inefficient design of the website. These kinds of security breaches have put the bank in financial, reputational and legal shock waves. It is time that banks should come up with some strong alarm so as to trace the attempts to hack. The systems which contain confidential matters must be properly guarded. Therefore, an adequate security mechanism is urgently needed. The banks have to cast light to the separation of internal systems and meagre internal security. The firewalls must be constructed among their various functioning systems. By constructing theses firewalls the external breaches could be minimized. However, the greatest risks are due to the employees of the organizations, who are the banks internal sources. The banks must develop security mechanisms which would act as a rigid wall to bar the cyber hunters from hunting their prey.

TECHNIQUES OF CYBER INFRINGEMENT

The 21st century can also be called as the internet era as the use of digital space is flourishing in all sectors. Once we start using internet and cyber space, there is no real exit as all our information is stored infinitely. The more the usage of digital space, the more is the threat to cyber security. On this wise, the electronic banking has proved to be an easy and lucrative target to the cyber fraudsters. The cyber-attacks on e-banking sector have increased rapidly in the recent years as the use of online banking systems by people has

increased only in the past few years. To reduce these threats and to safeguard customers the banks should adopt stringent cyber security systems and other preventive measures. But first of all, one should understand the types of cyber-attacks in e-banking sector for controlling them. In this chapter various types of cyber threats in e-banking sector are discussed.

1) Phishing

Phishing is one of the classic cyber-attack methods which use spoofed emails or messages that leads the user to infected websites to obtain the bank information from people such as account number, credit/debit card number, passwords, social security number, etc. These mails are designed to appear as authenticated ones so as to defraud people easily. Thus ultimately, the hackers can access the victim's bank account effortlessly.

2) Vishing

Vishing is a combination of voice and phishing where the cyber hunters use voice calls and represent themselves as the employees of banks and thereby make the bank's customers provide all the information related to their account.

3) Smishing

Smishing is a combination of SMS and phishing. It is more like of vishing, but here the cyber criminals collect bank information from the customers by sending SMS and making them believe it as authenticated message from the banks.

4) Watering Hole

Watering hole attack is merely a development from phishing attack. In phishing, the hackers attack people by sending spammed mails which connect people to infected websites whereas in watering hole the cyber attackers compromise a particular website and wait for people to access such websites. This type of attack targets only a specific group of people and the hacker has to wait for months after infecting such websites.

5) Pharming

The term pharming is derived from two words namely 'farming' and 'phishing'. Here the cyber criminals hack the URL of a bank website thereby redirecting such bank customer to a fake bank website. And it will be really difficult for the customers to differentiate between the original and fake website and so they usually end up providing their information in such websites. Hacking of a bank's URL can be done in two ways:

1. DNS Cache Poisoning
2. Hosts File Modification

6) Assault by Threat

When a person is threatened of his life through e-mails, messages or calls to give his bank details, it is known as assault by threat.

7) Credit Card Redirection

This is a new type of cyber-attack in e-banking which compromises the e-commerce websites thereby getting access to the credit card information of such website's users. Here, the credit card processing file is modified and the details of such credit cards are redirected to a phishing site during the payment process when used in the particular e-commerce website.

8) Triangulation

In this form of cyber-attack, the hackers create an infected commercial website providing huge number of discounts and free shipping of its goods. When an individual buys the products using the bank cards in such e-commerce sites, the hackers collect all the information of such cards effortlessly.

9) Malware Attacks

Malware is a kind of software that bugs a person's computer and spreads viruses through mails and social networks to other computers. This bug/virus will be controlled by the hacker and the information found in such computers will be compromised. This is one of the most dangerous cyber-attacks as this is mostly used for demanding ransom from individuals. So when this type of attack is made on a banking system, it ultimately compromises the customer's information available. Some of the most popular banking malware are Zeus, Carberp, Spyeye, Tinba, and the recent KINS. But surely, the first three agents are considered to be the most popular threats by the security community. Zeus is the oldest of them. Numerous variants were detected

during the last five years, and they have been often used to commit cyber fraud on a large scale. The first version of the Zeus Trojan was detected in July 2007, when it was used to steal information from the United States Department of Transportation [3]. This type of cyber-attack on the governments is said to be cyber warfare or cyber terrorism.

10) **Man in the Browser (MITB)**
Man in the Browser is a type of software or an infected code which attaches itself to the computers in banks and helps the hackers to modify the banking transactions of the people to their interests. This type of attack can be hidden from the victims and it will be very difficult for both the bank and the individual to figure out that such type of attack has been made.

11) **Salami Attack**
Salami attack is a sophisticated form of cyber-attack in banking sector, where hackers make small attacks which end up in accumulating a large amount of money in the end. It is also known as salami slicing. In banking sector, the attackers hack the bank accounts of people and deduct very minimal amount from it for a specific period of time. This makes the detection of such cyber-attack difficult and the bankers and victims are always unaware of such attacks.

IMPACTS OF CYBER CRIME

The digital era has proved to be of immense help for the growth of business organizations. Banking institutions being a lucrative business had to adopt digitization for promoting its business. While digitization has many benefits, it is not free from the dark side of cyber-crime. Since the banks have all the information of customers from personal identification to bank account details, it is easy for the cyber hunters not only to earn huge amount of money but also infringe the privacy of such customers by way of identity theft. Nevertheless, the impact of such cybercrimes still remains to be a nightmare. Some of the impacts of cybercrime are discussed below.

Financial Impact

It is a known fact that the main motive of cyber hunters is earning money. When the bank servers are hacked, it can result in huge monetary loss as they get all details including debit/credit card number with the Personal Identification Number (PIN). Not only this, the banks has to spend huge amount of money to identify the origin of such threat and recover from it.

Social Impact

The cyber-attacks not only result in financial loss but also creates a greater impact on the society. This is because when there is a cyber-attack, the customer loses trust over such bank which ultimately damages the reputation of the financial institution. This also results in loss of productivity and customer confidence of the banks.

CYBER SECURITY TRENDS IN INDIA

At present age, information is considered to be a valuable asset and storing of such information in data warehouses and clouds have made the work of service sectors easier. However, the development of cyber space poses a great threat to such information asset. And with the evolving concept of digitization, the information of every single person from physical address to social security number is available online. Therefore increasing the data security system in all the sector remains the sine qua non of protection of such valuable information. As for as the banking sector is concerned, ensuring the digital information security has become vital.

Indian banks are not an exception to these cyber frauds/attacks. Else, they prove to be a lucrative target for the cyber criminals as they provide for large amount of information data. On this wise, the central bank of India, i.e., The Reserve Bank of India, has issued certain guidelines regarding cyber security frameworks in banks through two notifications so far. The first notification was issued on April 29, 2011 by the Department of Banking Supervision regarding information technology, e-banking, technology risk management and cyber frauds [4]. It directed the banks to create a separate information security team to focus on the data security and cyber frauds. The circular also mandated the banks to have control over the access of IT data even by its

employees as the data can also be breached due to insider attack or espionage. It made the banks to assess the vulnerabilities soon after they find them and protect the data so as to avoid any form of cyber-attacks. Other security measures such as encryption, protection against malware, and developing robust firewalls were also provided in the circular. The report discussed about the awareness to be created among the employees regarding growing cyber threats and ways to track such cyber frauds.

Even with all the above-mentioned mandates and increased security levels by banks, the cyber-crimes were not under control as the technology used by the banks has further gained momentum. This made the RBI to issue another special circular on cyber security frameworks in banks on June 2, 2016 [5]. This circular mandated the banks to have a board-approved cyber security system and to give an immediate notice to RBI of the cyber-attacks, if any. The circular directed the banks to have a continuous surveillance over IT data and to create cyber awareness at all levels including top management authorities and stake holders. The banks were also directed to increase its defense levels in the cyber space.

Still, the cyber-attacks have not come down. As the technology develops, the landscape of cyber-crimes and cyber warfare are also increasing. Therefore, RBI has included cyber security measures in its agenda for the year 2018-19. Since the digital payments in the banking sector has gained popularity among the public, the RBI has decided to further strengthen and modify its encryption levels, cyber security and Know Your Customer (KYC) norms. The RBI report for 2018-19 said that "In order to secure consistency and improve the efficiency of the offsite monitoring mechanism, an Audit Management Application portal to facilitate various supervisory functions of the Cyber Security and Information Technology Examination (CSITE) Cell and to fully automate monitoring of returns has been envisaged, which will be operationalized by March 2019" [6].

The precautionary systems adopted by the banks in the recent years are as follows:

- Having a proxy server type of firewall so as to provide for high level of monitoring as there will be no direct connection between the internet and the bank's system.
- Usage of Secured Socket Layer (SSL) by the banks provides authenticated servers by using client side certificates issued by the banks. Nowadays most of the banks use 128-bit SSL for securing the online transactions and communications. In India, only SBI uses 256-bit SSL for protecting the communication servers.
- Having proper infrastructure for backing up of data by the banks is crucial.
- Record keeping of the online applications such as mobile banking apps in encrypted and decrypted form.
- Raising of the bar in cyber threats ultimately made Reserve Bank of India (RBI) realize the need for a holistic and integrated approach towards cyber security, resulting in which a circular from RBI inhibiting the guidelines on cyber security came into effect [7].

RECENT CYBER ATTACKS

- A recent survey in 2017 of more than 800 representatives from financial institutions worldwide found that a cyber security incident involving a bank's online banking services costs the organization $1.75 million on average. That is twice the cost of recovering from a malware incident, which average $825,000. The survey, conducted by Kaspersky Lab and B2B International, found that 61 percent of cyber security incidents affecting online banking come with additional costs such as data loss, loss of brand reputation, and confidential information being leaked [8].
- According to a recent survey by content delivery network services provider Akamai, India ranked fourth in the list of the top 10 target countries for Web Application Attacks. Another report shared by the Indian government mentioned that about 53,000 data and security breaches were reported last year across financial and government institutions [9].

SUGGESTIONS

Before 1980s, cyber-attacks were fewer in number and were committed by individuals, mostly by computer nerds who wanted to prove their knowledge. But in later years, the cyber-crimes became more organized and sophisticated as it was found to be a lucrative field for committing crimes. The shift from mischievous threats to properly organized and targeted attacks has created a greater concern among the organizations and governments worldwide. Hence, there is an exigency to address both security and privacy issues prevailing in the banking institutions.

Firstly, it is pertinent to understand that while launching of cyber-attack does not cost much, the identification of such crimes cost huge amounts of money. In the digitized and globalized world, any anonymous person can launch cyber-attacks on a banking institution in one country residing in a completely different place. This makes the tracking back of such attack difficult and costly. Thus, fighting such cybercrime single handedly is almost impossible. So the governments and business organizations across the world must work together and address this problem by way of regulating the cyber security in a cross-border or universal manner.

Secondly, while strengthening the cyber security is significant it is also important to sail safe in the cyber space. Awareness must be created among the customers regarding the cyber threats so as to protect themselves from the cyber hunters.

Thirdly, special legislations regarding cyber security in banking must be enforced. Not just enforcement, implementation of such laws is crucial thereby not only taking actions against cyber-attacks but also taking preventive measures before such attack is made.

Finally, special cyber cells dealing with the cyber-attacks must be organized in each and every bank so as to control the cyber threats. The only possible way to prevent the organized cyber-attacks is to have a cyber security mechanism in an organized manner.

CONCLUSION

Even though e-banking services in India have been gaining pace, the rate of adoption is still comparatively low considering the developed countries. The Indian banks have also invested huge amounts to boost the e-banking activities so as to facilitate the customers and in return get their loyalty towards the banks. Though there are various factors which restrict the customers from using e-banking services, the main concern remains the concern for security and privacy. In India, legislations which pertain to the security of e-banking are shed under the Information Technology Act, 2000 [8] and are scattered under the SEBI regulations, Reserve Bank of India's guidelines in order to safeguard privacy, especially online privacy, in electronic banking system. Moreover, the 2008 amendment of the Information Technology Act has provided special provisions under sections 43, 43A, 44, 66E, 67, 67A, 67B and few other sections which promote and protect data and privacy in online transactions. The e-banking services are mainly availed by the younger generation and even today the older generation feels the usage of e-banking to be a threat. E-banking services in the near future must be designed in such a way that irrespective of who the user is there shall not lay any sense of difficulty or dismay using these facilities. Though we talk about the infringement of privacy on the PDIs of the customers yet we have no means other than e-banking to transact in a speedy manner. Hence the government should come up with methods of securing the information and the people through various security mechanisms, which would protect the customers from threats of external source and it should also bring in penal/stringent provisions which would taunt the employees of the organization to take part in unscrupulous activities such as leaking of information, etc.

REFERENCES

1. Cambridge Dictionary, [cited 2018 Dec 18]; Available from: https://dictionary .cambridge.org/dictionary/english/electroni c-banking.
2. Thulani D, Tofara C, Langton R. Adoption and use of internet banking in Zimbabwe:

An exploratory study. *Journal of Internet Banking and Commerce*. 2009.
3. Modern Online Banking Cyber Crime. Infosec Institute. [updated 2013 Nov 5; cited 2018 Dec 18]; Available from: https://resources.infosecinstitute.com/modern-online-banking-cyber-crime/.
4. Department of Banking Supervision, RBI, Guidelines on Information Security, Electronic Banking, Information Risk management and cyber frauds. The Reserve Bank of India [updated 2011 Apr 29, cited 2018 Dec 18]; Available from: https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf.
5. Reserve Bank of India, Cyber Security Frameworks in India. The Reserve Bank of India [updated 2016 Jun 2, cited 2018 Dec 18]; Available from: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0.
6. PTI. RBI working on measures to further beef up cyber security in FY19. The ET. [updated 2018 Sep 3, cited 2018 Dec 18]; Available from: https://economictimes.indiatimes.com/news/economy/policy/rbi-working-on-measures-to-further-beef-up-cyber-security-in-fy19/articleshow/65656064.cms.
7. Reserve Bank of India's Guidelines on Cyber Security, https.in. [updated 2018 Nov 13, cited 2018 Dec 18]; Available from: https://www.https.in/blog/rbi-guidelines-cyber-security/
8. Goldman J. The price of a breach: Cyber-attacks on online banking services cost $1.75 million to resolve. eSecurity Planet [updated 2017 July 03, cited 2018 Dec 18]; Available from: https://www.esecurityplanet.com/threats/the-price-of-a-breach-cyber-attacks-on-online-banking-services-cost-1.75-million-to-resolve.html.
9. Pani P. Cyber-attacks on smaller banks likely to double, say experts. Business Line, The Hindu [updated 2018 Aug 17, cited 2018 Dec 18] Available From: https://www.thehindubusinessline.com/money-and-banking/cyber-attacks-on-smaller-banks-likely-to-double-say-experts/article24718715.ece.

Cite this Article
R.B. Rishabh, B. Yamuna Saraswathy. Flaws in E-Banking: A Prey to Cyber Hunters. *National Journal of Cyber Security Law*. 2018; 1(2): 8-15p