DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume I Issue X is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner whatsoever for any consequences for any action taken by anyone on the basis of information in the Journal.

Copyright © International Journal for Legal Research & Analysis
EDITORIAL TEAM

EDITORS

Ms. Ezhiloviya S.P.
Nalsar Passout

Ms. Priya Singh
West Bengal National University of Juridical Science

Mr. Ritesh Kumar
Nalsar Passout

Mrs. Pooja Kothari
Practicing Advocate

Dr. Shweta Dhand
Assistant Professor
ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS
ISSN

2582-6433 is an Online Journal is Quarterly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN

2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.
## INDEX

1. Abstract ........................................................................................................ 1
2. Introduction ...................................................................................................... 2
3. History of Trans-genders in India ................................................................. 3
   - Mythology
   - The Vedic Period
   - 1526-1748
   - 1643-1680
   - 1860-1935
4. Social barricades ............................................................................................. 5
   - Exclusion within the family
   - Harassment of Transgender Students in Schools
   - Weak economic status
   - Victims facing crimes and violence
5. Judicial progress pertaining to Trans-rights ................................................... 8
   - Queen Empress v. Khairati (1884)
   - National Legal Services Authority v. Union of India (2014)
   - Justice K.S. Puttaswamy v. Union of India (2017)
   - Navtej Singh Johar v. Union of India (2018)
   - Arun Kumar v. Inspector General of Registration, Tamil Nadu (2019)
   - Hina Haneefa @Muhammed Ashif Alin v. State of Kerala (2021)
6. Statutory development through years .............................................................. 12
8. State trans-upliftment ...................................................................................... 16
9. Conclusion ........................................................................................................ 17
Cyber security in financial institutions in India: A critical analysis

Abstract

We are living in modern world or we can say digitalised and globalised world. Where things are fast and convenient but this convenience has cost. E-Banking has provided us many things but is not free from difficulties or problems. One such problem is ensuring the cyber security in the financial sector. This paper discuss various dimension of cyber threat. Regulatory framework for cyber security available in India. This paper provides some insight into the question that do we need specific legislation for cyber security in India.

Introduction

What is cyber security?

Cyber security\(^1\) is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It’s also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

- **Network security** means computer network from hackers, whether targeted attackers or opportunistic malware.

- **Application security** protects software and devices from threats. A compromised application could provide access to the data it’s designed to protect.

- **Information security** protects the integrity and privacy of data, both in storage and in transit.

- **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

- **Disaster recovery and business continuity** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data.

- **End-user education** addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

\(^1\) Kapersky.co ( march 2 2021) (https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security)
Why cyber security important in financial sector?

(By: Prabhat Singh)

Financial institutions are backbone of any economy. Like banks, NBFCs, payment banks etc. they enable the people of any country to do business seamlessly and play a mediator role between business. banks also provide saving option for general people. After globalization and computerization in early 1990s, nature of transactions changed drastically like now we do not go to branch and fill the receipt to withdraw money, we go to ATM and withdraw money very easily and if we want transfer money, we can send it through net banking to anyone anywhere in the world just simply putting user id and password. A very recent invention in this is UPI, many merchants are using this nowadays for receiving money from mobile wallet. All these technologies eased the process of transaction for business entity, merchants and for general people as well. But these technologies are susceptible to many hackers who do not rob the banks by gun or by attacking bank employees but they more sophisticated weapons viz software programme, digital algorithm etc. everyday new technology, new software are coming in the market which gives hackers new arsenal everyday.

Famous Bangladesh bank cyber heist took place in February, 2016. In this heist perpetrators managed to get access to the bank’s credential anyhow and used that credentials for making almost thirty-five request to the federal reserve bank of New York for transferring the funds to accounts in Philippines and Sri Lanka. 2016 attack was not the first of its kind before it Sonali bank of Bangladesh was also hacked in which perpetrators managed to remove US$250,000. From this case we can conclude that though e-banking is easy, fast, and efficient but there is risk involved. now we will try to understand that what is e-banking? And what dimension it holds?

Meaning of E-banking

E-banking is product which provides fast, easy and efficient electronic service that enable us access to bank account and to do online banking 24 hours a day, and 7 days a week. various dimension that e-banking holds-

- Safety – it is most important dimension because before using the e-banking user needs to trust e-banking system.
- Efficiency – e-banking system must be robust to handle the heavy load
- Ease of use – system should not be complicated, so that general people can use it properly.
From above mentioned dimensions, safety is the most important because if people found that system is not secure, they will not trust on that system in fear of loss of their hard-earned money.

**Cyber threats to banks and other financial institutions**

According to ‘B.R.Sharma’² The main types of e-bank frauds include:

1. Cheque Truncation System (CTS) Frauds
2. Identity Theft Phishing
3. Tele-marketing Frauds
4. ATMs Frauds
5. Debit and Credit Card Frauds
6. Internet Banking Frauds
7. Mobile Banking Instrument Frauds
8. Wire transfer, EFT/NEFT (Electronic Fund Transfer/National Electronic Fund Transfer) Frauds
9. Banking Social Engineering Frauds
10. Colour photo copier Frauds
11. Unauthorised Reversals
12. Vishing
13. Skimming
14. Salami Frauds
15. Money Laundering
16. Diversion of electronic documents, messages, etc. from the right addressee to someone else.
17. Misappropriation of deposit(s) from the account of a customer to the account of the fraudster.
18. Corruption, deletion or theft of command protocol, data or software.
19. Induction of illegal and unauthorized commands and instructions for personal gains.
20. Deletion of incriminating record relating to withdrawal (or deposit) in the computer.

² BR Sharma, Bank Frauds Prevention & Detection, chp4.2(4th ed,2016)
21. Corruption of computer to stop functioning, through virus or command. 
In General integrity, secrecy and security of the electronic 
document, message, data, etc. is compromised.

1. **Cheque Truncation System (CTS) Frauds**
   
   Chaque truncation system is an online image based cheque clearing system. Through creating 
a fake image, hackers draw money from banks. There are mainly two type of cheque fraud – 
1- Counterfeit checks – imitation of original check created by scan and print 
2- Altered checks- modification of genuine instrument by altering and writing the new 
content with a fake sign near it

2. **Identity theft phishing**
   
   In identity theft cyber criminals send fake emails to people purporting to be from legitimate 
bank or financial institutions and lure through mail to click a fraudulent link and ask information 
like pin, account- number, password etc. After obtaining such information cybercriminal 
withdraw or transfer money from your account.

3. **Tele-marketing frauds**
   
   Tele-marketing fraud happen over phone calls. Telemarketer call to the victim and tell story 
like you have won lucky draw coupon or lottery or any other free gift or money and ask 
information as ATM card no. and password or any information through which they can 
withdraw money. In this way telemarketer ask the victim to take immediate decision. Often 
in such situation people give them information then tele marketer withdraw money and cut 
the calls. Tele-marketing frauds happening in huge numbers in India especially people from 
rural background often become victim of tele-marketing fraud.

4. **ATM frauds**
   
   ATM frauds occurred via ATM machine by stealing someone else ATM card ATM card data. At 
present there are four ways through which ATM fraud can happen-
1. Card Shimming- It is done by a device which is installed on the ATM for gathering data 
   from card.
2. Card Skimming- In this card is imitated by stealing the electronic data of card. Victim 
even don’t realize this until money is withdrawn from their account.
3. Card Trapping- it is done through installing a device on the ATM and then card trapped in ATM machine. When victim go out from ATM to get help then trapper enter in ATM and withdraw money.

4. Jamming of keyboard- This is done by jamming important keys in the ATM machine and when transaction got failed and customer go out of ATM then fraudster enter and withdraw money immediately.

5. **Debit and credit card fraud**

   It includes fraud like cloning, cyberstalking, identity theft, email spoofing etc.
   1. Debit card fraud- debit card fraud occurred when someone got your debit card number and personal identification number (PIN) and use it to withdraw money or online purchase.
   2. Credit card fraud- it occurs when someone steal your card or got access to your credit card number, PIN, Security code and make unauthorized transaction by using that information.

6. **Internet banking fraud**

   Generally, bank provides user id and password to the customer in order to facilitate internet banking to them but sometimes due to silly mistakes fraudster got this id, password through which they transfer money to their account.

   According to financial express \(^3\) in frauds related to debit card, credit cards and internet banking, Rs 129 crore has been lost in just three months to December 2019. A total number of 21,041 such cases were registered in these three months, Anurag Thakur, MoS, ministry of finance said in to a question in Lok Sabha.

7. **Mobile banking instrument fraud**

   Nowadays mostly people use mobile banking for retail purchase and transferring money to others. Mobile banking fraud committed via device theft or by automated attacks caused by malware, bots and emulators which results into account takeover, carrier data breaches etc.

8. **Wire transfer, EFT / NEFT (electronic fund transfer/ national electronic fund transfer) frauds**

   Sending money from one place to another through electronic means is called electronic fund transfer. In India it is called national electronic fund transfer. To do fraud by this means all

---

required that is password and operating key. Often frauds are committed by operator or programmer or by outside fraudster with help of these persons.

NEFT is also used for terrorist funding and by HAWALA people to do money laundering because through NEFT recipient just get name and amount.

9. **Banking social engineering frauds**
Social engineering fraud committed via social media. In this criminal use social skills to manipulate the psychology of victim. Through lies they construct a story which look realistic to either scare or excite the victim and hope that victim will provide them sensitive information.

10. **Colour photo copier frauds**
This could be modus operandi for fraud because every time when we do print, scan or fax from machine, it creat and save the image of document in the hard drive.

11. **Unauthorized Reversals**
A request for bank transaction reversals made to system like Paypal because of suspicion of unauthorized use of bank account.

12. **Vishing**
Vishing is actually combination of voice and phishing. Fraudsters call the victim and act like representative of your bank and ask information like password, user id etc. And then transfer money from victim’s bank account.

13. **Skimming**
It is a form of white-collar crime. In which earned money is not accounted. It is done to cheat partner or evade tax.

14. **Salami frauds**
This is also called salami slicing. In this scammer withdraw small or very little amount of money for example Rs 4 which is not noticed by account holders or if notice then ignore because it is insignificant amount to do the complaint. But number of accounts is big like if 1 million account is involved then scammer got 4 million rupees in his account just by withdrawing so little amount. It is often unnoticed by account holders as well as banks.
15. *Money laundering*
Money laundering is not new. Launderers always try to convert black money into legitimate money now cyber world provides various ways for money laundering like by identity theft they can use someone else account to transfer the money and make it legitimate or by online gambling or via international wire transfer.

16. *Diversion of electronic document, messages etc. from right addressee to someone else.*
In this one fraudster help other by knowingly making a mistake. Give sensitive information to fraudster.

17. *Misappropriation of deposit from the account of a customer to the account of fraudster*  
In this insider in bank do this with the help of outside fraudster. It is also done by hacking the bank system.

18. *Corruption, deletion or theft of command protocol, data or software*  
This is done through intrusion in system by virus or malware or trojan. It is like making some command to SWIFT or Paypal for transferring fund illegally.

19. *Induction illegal and unauthorized commands and instructions and instruction for personal gains*

20. *Deletion of incriminating record relating to withdrawal (or deposit) in the computer*

21. *Corruption of computer to stop functioning through virus or command*  
It is also called distributive denial of service. In which many commands were originated at the same time to stop the functioning of system.

These crimes are new by nature and scope. These crimes are of different nature so investigation of these crimes is also difficult. According to B.R. Sharma⁴ The main features of these frauds are:

- No eye-witnesses,
- No familiar crime scene,
- No usual evidentiary clues,
- No documentary evidence worth the name,
- The data in the computer is misused, may have been erased.

The investigating officer is not familiar with the type of evidence found in E-banking frauds. If he is to meet the challenges of investigation, he needs working

---

knowledge of the computer technology and has to update it continuously, as it is changing very fast. It is difficult for the normal investigating officer to do so.

**New cyber threats emerging during Covid pandemic**

During pandemic period we are facing enormous problems, like lockdown has been implemented for many months. People got stuck in home so new work culture has been developed which is named ‘work from home’. Which leads to rapid digitalisation of banks also, people started using online payment through mobile wallet like PAYTM, PhonePe, etc. due to ‘social distancing norms’ and in fear of corona virus.

So rapid digitalisation leads to rise in the numbers of cyber- crimes. According to KPMG\(^5\) banking clients have reported significant increase in ‘phishing email’ about COVID-19 to the customers. There is also rise in the no. of ‘call centre’

Due to rise in the numbers of cyber- attacks from hostile countries like china and Pakistan in the wake of pandemic, Indian government is planning\(^6\) new cyber security system for financial sector. At present Indian computer emergency response team [ CERT-IN] handles all cyber security risk. There is discussion for new agency CERT-FIN which will be dedicated to financial sector and handle cyber threats to financial sector. According to proposal CERT-FIN will call expert from ministry of corporate affairs, the employees provident fund organization, the serious fraud investigation office, the security printing and minting corporation of India limited and the goods and service tax network.

Cyber criminals creating new websites on the name of term like COVID, Coronavirus news, corona map etc. and when someone click on that link, malware, ransomware or trojan automatically downloaded in their system through which cyber criminals steals sensitive information from victim’s computer or smartphone.

**Cyber laws and policy for cyber security in financial sector**

**Cyber laws** –

With respect to cyber laws, the most important law is Information Technology Act, 2000. The

---


\(^6\) [ Rajeev Jayaswal ], [Govt plans cyber security system for financial sector ], [ Hindustan times.com], [ Jan 16 2021, 12:30 pm ], [ https://www.hindustantimes.com/india-news/govt-plans-cyber-security-system/story-bHRwwBeFVGLIrA3VMmOaDO.html ]
objectives of this act are as follows\textsuperscript{7}, stated in the preface of the act itself.

“An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as —electronic commerce, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker’s Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.”

This act provides legal recognition to electronic record as well as there is provision for civil and criminal liability for cyber-crime like—

Section 43\textsuperscript{8} in which there is provision for civil liability regarding data theft or damage to computer or computer system. This is the first legislation in India which deal with the issue of data theft. Provision for criminal liability regarding data theft is in section 65 and 66.

the employees’ liability in an organisation which is sued against for data theft or such offences and the amount of responsibility of the employer or the owner and the concept of due diligence were all debated in the first few years of ITA -2000 in court litigations like the bazee.com case and other cases. it felt that corporate liability should be taken seriously regarding data theft.

Subsequently section 43-A\textsuperscript{9} was inserted by information technology amendment act 2008 in which there is provision for compensation in case of failure to protect data. corporate responsibility was ensured and in this way business entities under legal obligation to protect sensitive personal data of consumers. Further what is sensitive personal data has since been clarified by the central government vide its Notification\textsuperscript{10} dated 11 April 2011 giving the list of all such data which includes password, details of bank accounts or card details, medical records etc.

After this notification awareness increased among various financial institution who are dealing in technology- based banking. General awareness also increased for data privacy.

Now it become mandatory to comply rules stated in central government notification dated on April 11\textsuperscript{th} 2011. Any breach results into claim of compensation which results into financial as well as reputational loss.

Section 65\textsuperscript{11} there is provision related to tampering with source document. Computer source

\textsuperscript{7} Information technology act ,2000, Acts of parliament, no. 21,2000 (India).
\textsuperscript{8} Information technology act,2000, § 43, Acts of parliament, no. 21, 2000 (India).
\textsuperscript{9} Information technology act,2000, § 43-A, Acts of parliament, no.21, 2000(India)
\textsuperscript{11} Information technology act,2000, § 65, Acts of parliament, no. 21, 2000 (India).
code under this section means computer commands, design, layout etc.

**Section 66**\(^12\) it deals with computer related offence. Data theft, given under section 43 leads only to civil liability and compensation of damages but in this it leads to criminal liability and imprisonment upto three years or five lakh rupees fine or both.

After information technology amendment act, 2008 the word “hacking” is removed because of ethical hacking academic programmes. And in same amendment section 66 is widened.

**Section 66A**\(^13\) it deals with issues like email spoofing or sending offensive messages or mislead or deceive the recipient or annoy him through communication services. Punishment of imprisonment upto three years or fine or both are prescribed in this section for these crimes.

**Section 66B**\(^14\) deals with dishonestly gaining stolen computer resource or communication device. This section mentioned punishment of imprisonment upto three years or one lakh fine or both.

**Section 66C**\(^15\). It deals with the crime of identity theft like using someone else’s user id and password without his consent or authority and making fraudulent transaction by that. It is punishable by 3 year imprisonment or one lakh rupee fine or both.

**Section 66D**\(^16\) Cheating by personation using computer resource or a communication device shall be punished with imprisonment of either description for a term which extend to three years and shall also be liable to fine which may extend to one lakh rupee.

As cyber-crime is of global nature. Keeping this in mind it is necessary to discuss **section 75**\(^17\) which says that the Act applies to offences or contravention committed outside India, if the contravention or the offence involves a computer or a computer network located in India.

Above mentioned laws provide for penal as well as civil provision but there is lack of special legislation regarding financial institutions. In case of vishing of telemarketing frauds people don’t know whom to approach, banks do not help the victim they just said that you should not give your credential to anyone or you should secure your system but there is no provision for reversal of money in case of fraudulent transactions if it is in place then bank employee does not follow that.

**RBI** also does not provide any mechanism to grant the relief to victim of identity theft or vishing or telemarketing frauds. Many rackets are operating as call centre in India.

At times it has been observed that enforcement


\(^{13}\) Information technology act, 2000, § 66A, Acts of parliament, no. 21, 2000 (India).


\(^{15}\) Information technology act, 2000, § 66C, Acts of parliament, no. 21, 2000 (India).

\(^{16}\) Information technology act, 2000, § 66D, Acts of parliament, no. 21, 2000 (India).

\(^{17}\) Information technology act, 2000, § 75, Acts of parliament, no. 21, 2000 (India).
agencies have not proper tooth to fight cyber-crimes in financial sector. Question here is that do we need specific legislation for cyber-crimes in financial sector? This question involves critical analysis because having a specific legislation on central level has merit and demerit both. Specific may be too prescriptive, that it can fall behind the constantly evolving cyber-crimes. **RBI Policy**- RBI notification\(^\text{18}\) dated on June 2, 2016 says that Banks should put in place a cyber-security policy elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk, duly approved by their Board.

It also says that testing for threats or vulnerabilities should be done at reasonable intervals and for this security operation centre must be setup. It also urge that a cyber crisis management plan must be prepared and approved by board and cyber crisis management plan should include four aspect –

1. Detection  
2. Response  
3. Recovery  
4. Containment  

In addition to this RBI says that cyber resilience framework should be assessed and indicators must be developed to asses the risk preparedness. Realizing that cyber threat can be originate from anywhere RBI urges to the banks that bank should create awareness among staff at all level and it also require that top management and board must have sufficient awareness and knowledge of some fine nuances of threats. It also says that bank should proactively promote awareness among various stakeholders like consumers, vendors, service providers, etc.

**RBI issue guideline for online banking and using mobile wallets and prepaid payment instrument for example** RBI guidelines dated on Jan 4 2019\(^\text{19}\) says that –

i. The SMS alert for any payment transaction in the account shall mandatorily be sent to the customers and e-mail alert may additionally be sent, wherever registered. The transaction alert should have a contact number and / or e-mail id on which a customer can report unauthorised transactions or notify the objection.  

ii. Customers shall be advised to notify the PPI issuer of any unauthorised electronic payment transaction at the earliest.

---

\(^{18}\) [RBI.org.in], [https://www.rbi.org.in/Scripts/NotificationUser.aspx?id=10435&Mode=0]  
\(^{19}\) [ rbi.org.in], [https://www.rbi.org.in/Scripts/NotificationUser.aspx?id=11446&Mode=0] (Jan 12 2021)
iii. To facilitate this, PPI issuers shall provide customers with 24x7 access via website / SMS / e-mail / a dedicated toll-free helpline for reporting unauthorised transactions that have taken place and / or loss or theft of the PPI.

iv. Further, a direct link for lodging of complaints, with specific option to report unauthorised electronic payment transactions shall be provided by PPI issuers on mobile app / home page of their website / any other evolving acceptance mode.

v. The loss / fraud reporting system so established shall also ensure that immediate response (including auto response) is sent to the customers acknowledging the complaint along with the registered complaint number.

In addition to this RBI also says that if any unauthorised transaction happen due to negligence by customer like if customer has shared his account’s login id and password to someone else then loss will be suffered by customers and institutions have zero responsibility in this scenario.

By observing above mentioned laws and policies we can classify cyber security measure and possible remedies and responsibilities at two level-

1. On institutional level
2. On customer level

Now we will critically analyse preventive as well as remedial measure present at both level.

1. On institutional level- To understand the preparedness and preventive measure we will look into STATE BANK OF INDIA’s policy and guidelines.

When we look at the information security manual\(^{20}\) of the bank we found following observation-

- It says that CIA (Confidentiality, integrity, availability) is their true spirit. Bank employees should maintain that because any compromise in CIA would result into negative feedback, criticism by media, and penalty.
- It says that bank has internal mechanism to monitor the activities of user means bank employees, investigation and to catch the culprit.
- It also urge that bank has information security framework approved by the board and which is reviewed by the same periodically.

\(^{20}\)[SBI.co.in], [https://sbi.co.in/webfiles/uploads/files/28052019_IS_Manual.pdf], [Jan 13 2021]
- It also says that state bank security operation centre has been setup for real-time monitoring, analysis, correlation and incident management.
- It also lay down that bank runs security programmes for awareness among its staff.
- It also say that bank spread awareness among customer through advertisement.

From above mentioned policies we can conclude that preventive measures are in place. For detection, recovery and investigation bank needs to put an emergency response team.

In the Deloitte’s 2020 global risk management survey\(^{21}\) Sixty-seven percent of respondents named cybersecurity as one of the three risks that would increase the most in importance for their business over the next two years, far more than for any other risk. Yet, only about one-half of the respondents felt their institutions were extremely effective or very effective in managing this risk.

Another problem which I can see that there is no mechanism for independent assessment of cyber resilience framework of banks and security capabilities of third party like payment gateways. On top of this there is no clear responsibilities and accountability at banks.

On customer level- for customer awareness RBI and various banks advertise the guidelines and ask the customer to not provide sensitive information to any one whether he is bank official or relative or government representative.

For example- SBI in its online banking terms of service it says that The USER shall:

1. Keep the User-id and password totally confidential and not reveal them to any third party.

2. Create a password of at least 8 characters long and shall consist of a mix of alphabets, numbers and special characters.

3. Commit the User-id and password to memory and not record them in a written or electronic form

4. Not let any unauthorized person have access to his computer or leave the computer unattended while using Internet Banking Services.

5. Not disclose/reveal his/her personal or confidential information to anyone over email/SMS/phone call even if its purportedly from State Bank of India.

6. Not access OnlineSBI if his/her computer device is not free of malware (Viruses, Trojans, etc.).

Above mentioned guidelines can be seen in every other bank’s ‘terms of service’ and almost same guidelines have been issued for mobile banking or credit and debit card use.

Though banking app use SSL encryption yet many times these apps initiate non-encrypted transaction which is susceptible to web interface which make these apps vulnerable.

Another drawback present at customer level is that often people use same password for many website- like using same password for email, Facebook, online banking and other places. If someone has detected your Facebook- password then other things also compromised. According to a survey\textsuperscript{22} of consumer password habits from 2012, sixty-one percent of consumers reuse passwords among multiple websites and forty-four percent of consumers change their password only once a year or less.

At customer level no remedial plan is available to the customer often they lost money by being victim of tele marketing frauds, vishing etc.

---

\textit{way forward and conclusion}

\textbf{way forward-}

- For cyber-crimes there is only one legislation in India that is information technology act,2000. India needs standard and universal legislation to fight cyber- crimes in financial sector.

- An agency should be setup at central level to assess the soundness banks cyber security by using threat-intelligence. In threat-intelligence simulated cyber attacks were done to test a bank’s cyber security.

\textsuperscript{22} Id.at 17
• Cyber intelligence sharing platform should be developed between various agencies and banks.

• Cyber event should be ensured in banks like RBI has also made regulation about it.

• Bank should promote cyber security awareness among staff as well as consumers.

• Thematic review of Security capabilities of third-party providers must be done.

• Bank should produce its intelligence detection and response report.

### Conclusion

India is a developing country. Its institutions are evolving in every aspect and so can be said with respect to cyber security. Cyber security needs to be dynamic and resilient. There is no single technology or framework that can ensure cyber security in the modern era.

Indian banks have digitalised themselves. Customer can do banking via laptop or mobile phone or by cards any time anywhere. It is necessary to assure customer that their money is safe and the platform or app they are using for banking have proper security measures.

New technologies are evolving and financial institution cannot keep themselves aloof from these technologies because this is demand of the time but before launching the new cyber products for public bank must review safety measure and must ensure the customer about it.

Only banks or other financial institution do not owe the duty of cyber security. Consumer also has to play important role regarding cyber safety. As an aware consumer it is his duty to keep his devices virus or malware free and scan the devices periodically. He has to install a antivirus in all devices and should not install apps from unsecure server or links. Any unauthorised transaction known to consumer must be reported by him to relevant authority in financial institutions. We don’t have any cent percent secure plan or strategy but we can reduce the risk by being alert.