Management of Risk Issues in E-Banking – A Case Study

G Sravanthi

Assistant Professor, Department of Commerce & Business Management, Vaagdevi Degree & PG College, Kishanpura, Hanamkonda, Warangal District Telangana State – 506009

Abstract: **The people dependence on advancement of technology has enabled huge benefits and also lead to various new ways of technology based crimes where the people have been facing upon. Rising consumer dependence on rapidly changing advancements in the technology has created ways for misuse. The e-banking which is one of the sophisticated services of banks to its consumers have facilitated wide range of e-services at the finger tips of the consumers. The increasing use of e-banking by the people also resulted in increasing threats over the applications and programmes which further resulted in risks in performing e-banking transactions. Several risks have created the dilemma over the consumers of e-banking services. The present paper will throw light on the various risk factors and issues involved in e-banking transactions and further the study will provide the remedies that help to enable the risk free and error free supporting system for the e-banking operations.**

Key words: Compliance risks, EFT, hacking, KYA, Operational risks

I. OVERVIEW AND GROWTH OF E-BANKING

Indian economy is witnessing stellar growth over the last few years. There have been rapid developments in infrastructural and business front during the growth period. Internet adoption among Indians has been increasing over the last one decade. Indian banks have also risen to the occasion y offering new channels of delivery to their consumers.

Though the banking system in India has emerged in the last decades of 18th century but it has transformed to traditional operations to most advanced operations to the consumers. The commercial banking has started to receive new shape with the advancements of technology-enhanced products and services from 1980s. The banks in order to provide healthy transactions and to reduce their overburden and costs started to concentrate on the technology enabled services. As a result, multi-function ATM, Tele-banking, electronic transfers and e-cash cards were entered in the market. The growth in the use of internet has provided the facility of introduction to the e-banking transactions. The restricted services of banks were replaced with that of "anytime/anywhere/any how" type of services. The traditional banking system of providing service to person-to-person is replaced with many services under a single click concept. The customized tailor made services for satisfying the customer needs have recognized from the inception of e-banking.

The IT revolution had a great impact in the Indian banking system. The use of computers had led to introduction of online banking in India. The use of the modern innovation and computerization of the banking sector of India has increased many folds after the economic liberalization of 1991 as the country's banking sector has been exposed to the world's market. The Indian banks were finding it difficult to compete with the international banks in terms of the customer service without the use of the information technology and computers.

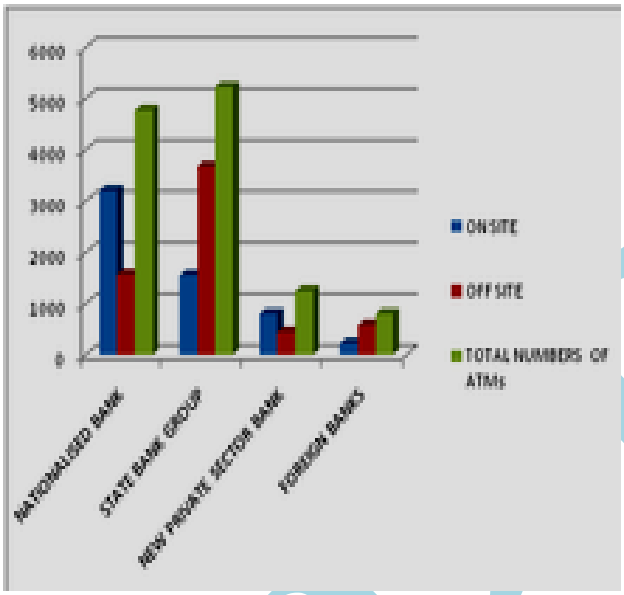
The RBI in 1984 formed Committee on Mechanization in the Banking Industry (1984) whose chairman was Dr C Rangarajan, Deputy Governor, Reserve Bank of India. The major recommendations of this committee was introducing MICR Technology in the all the banks in the metropolis in India. This provided use of standardized cheque forms and encoders.

In 1988, the RBI set up Committee on Computerization in Banks (1988) headed by Dr. C.R. Rangarajan which emphasized that settlement operation must be computerized in the clearing houses of RBI in Bhubaneshwar, Guwahati, Jaipur, Patna and Thiruvananthapuram. It further stated that there should be National Clearing of inter-city cheques at Kolkata,Mumbai,Delhi,Chennai and MICR should be made Operational. It also focused on computerization of branches and increasing connectivity among branches through computers. It also suggested modalities for implementing on-line banking. The committee submitted its reports in 1989 and computerization began form 1993 with the settlement between IBA and bank employees' association.

IN 1994, Committee on Technology Issues relating to Payments System, Cheque Clearing and Securities Settlement in the Banking Industry (1994) was set up with chairman Shri WS Saraf, Executive Director, Reserve Bank of India. It emphasized on Electronic Funds Transfer (EFT) system, with the BANKNET

communications network as its carrier. It also said that MICR clearing should be set up in all branches of all banks with more than 100 branches.

Committee for proposing Legislation On Electronic Funds Transfer and other Electronic Payments (1995) emphasized on EFT system. Electronic banking refers to doing banking by using technologies like computers, internet and networking, MICR,EFT so as to increase efficiency, quick service, productivity and transparency in the transaction.



Apart from the above mentioned innovations the banks have been selling the third party products like Mutual Funds, insurances to its clients. Total numbers of ATMs installed in India by various banks as on end March 2005 is 17,642. The New Private Sector Banks in India is having the largest numbers of ATMs which is followed by SBI Group, Nationalized banks, Old private banks and foreign banks.

The total off site ATM is highest for the SBI and its subsidiaries and then it is followed by New Private Banks, Nationalized banks and Foreign banks. While on site is highest for the nationalized banks of India. Branch banking in India has fallen by 15% with the success of Internet banking, according to a study by global consulting firm McKinsey & Company. According to the McKinsey survey, as many as 7% of the account holders in India are using the Internet for their banking needs. Internet banking use has seen a massive rise in the 2010-11 survey, taking the overall number of bank consumers who use the Internet to close 7% of the total bank account holders.

In 2007, the percentage of online users of banking transactions was just about 1%. In 2007, the number of times Indian respondents visited bank branch for doing transactions was 0.58 while the same in 2011 was 0.49, showing a fall of 15 percentage points. Branch usage has dropped by 27% on an average across Asia between 2007 and 2011, while usage of the Internet and mobile banking have increased by 28% and 83%, While there was a 15% decline in branch usage here, the growth in usage of the Internet and mobile banking has almost tripled. The average number of banking relationships across the country rose 19% from 1.4 in 2007 to 1.7 in 2011, while the average percentage of people willing to shop around rose 15, marking a greater willingness of consumers to vote with their feet and engage with a broader variety of financial institutions. The emerging trends point to a future where Internet will take center stage as the primary medium of product development.

II. STUDIES ON RISK ISSUES IN E-BANKING

E-banking has much future that facilitates the consumers to perform wide variety of financial transactions on a secure website operated by their online account system. The e-banking can perform many services including transactional, payments to third parties, fund transfer to any where in the world through online and investment purchase. The e- banking has facilitated with advanced characteristics than the traditional banking operations. The e- banking has witnessing the unprecedented speed of technological change. The e-banking is able to provide the product and service innovation due to changing customer expectations. The e-banking has also resulted in the increasing dependence of banks on third-party service providers.

E-banking is one of the forms of e-commerce. E-banking is simply the provision of information about a bank and its services via a home page on the World Wide Web (WWW). E-banking is also referred with easy, exciting, and empowering. It includes all financial services by an organization to its consumers who may be individuals or other businesses.

The e-banking has provided many advantages and at the same time because of its limitations and risks including proliferation of threats and vulnerabilities in publicly accessible networks it has put question marks over its trust and performance. The various developments and risk issues have given the initiation to Basel Committee to made study on banking supervision – risk management implications in the year 1998. The study is based on the risk implications of e-banking and e-money transactions. The study demonstrated that clear need for more work in the area of e-banking risk management, and that mission was entrusted to a working group comprised of bank supervisors, and central banks, the Electronic Banking Group (EBG), which was formed in November, 1999.

The EBG also has studied the traditional banking risks in light of e-banking capabilities. The study given that while not creating any inherently new risks, the e-banking increased and modified some of these traditional risks. The impact is more profound in strategic,

operational, legal, and reputation risks there by influencing the overall risk profile of the banking institution.

III. OBJECTIVES OF THE STUDY

The study mainly focuses on the following objectives.

1. To present the overview of e-banking frauds in India in the last 5 years.
2. To examine the risks involved in e-banking system in India.
3. To study the approaches for secured e-banking services for enabling sustainability.

IV. METHODOLOGY OF THE STUDY

The study is mainly based on the Secondary data sources which include the references of applications of software, reviews and reports on e-banking frauds generated by ASSOCHAM, internet and news papers. The primary data is collected through interview with bank personnel and the consumers who are performing e-banking transactions.

V. RISKS IN E-BANKING SYSTEM

Around 65% of the total fraud cases reported by banks were technology-related frauds (covering frauds committed through/ at an internet banking channel, ATMs and other payment channels like credit/debit/prepaid cards), whereas advance-related fraud accounted for a major proportion (64%) of the total amount involved in fraud.

From the field based observations and consulting with various personnel performing operations in select banks functioning in the state of Telangana, the following key observations are made on the various risks involved in e-banking system.

a). Operational Risks

The study clearly pointed out the likelihood of the operational risk that can emerge from the online banking can be compared to traditional banking. The banking environments which is converted to more systematic and complex by the day due to technology developments has led to many problems for the existing employees who were not in a position to go along with the technology. The internal and external fraud due to the loop holes in the technology implemented and used for transactions has led to increasing frauds by the bank employees in the recent past. The lack of training and development programmes to the existing employees putting the question marks over the speedy settlement of transactions.

The misuse of confidential information, damage to files which are saved in the folders of the various files, business disruption and system failures, failed or erroneous transaction processing, failed outsourced processes were some of the critical operational risks which the online banking is facing from years. The increasing operational risks may give advantage to the persons who are having technical expertise in online banking and thus lead to the mis use of the funds of the banks and as well of the consumers. Even till now, all the banks operating in India are not computerized. The use of online services in banking sector is still lacking in majority of the rural bank branches because of lack of exposure and infrastructure. Further, the banks' own adoption of technology for internal control and fraud risk management is still a far reach due to lack of frequent development programs for the bankers towards facing the customer complaints, KYC checks, customer data integration and fraud risk management. The following table shows the e-frauds which have been recorded during NEFT/RTGS transfers happened in the last 5 years. Table-1 clearly witness the raising fraud transactions under NEFT/RTGS platform and gives a clear view on the raising frauds happening in online platform.

Table 1: e-fraud statistics

Sl.No.	Period	NEFT/RTGS transactions resulting in fraud
1	2010-11	0.25
1	2011-12	0.60
2	2012-13	0.70
3	2013-14	0.80
4	2014-15	0.85

Source: ASSOCHAM report on e-frauds, 2015-16

b). Compliance Risks

One of the limitations for the e-banking services are the compliance risk which may arise from non-conformance with, laws, rules, regulations, prescribed practices, or ethical standards. It also arises when the legal rights and obligations of parties to a transaction are not well established.

Non-compliance results in serious consequences, including rating downgrades, regulatory enforcement actions and monetary fines, enforced suspension of operations, reputation damage, and in extreme cases, withdrawal of authorization to operate. The current e-banking system is still suffering from the cross border transactions and the compliance function still complicated due to the lack of jurisdictional clarity.

The following section provide the pattern of frauds that have been rising in Indian banking sector.

The statistics presented in table-2 shows the highest percentage of frauds happening in the internet based banking and ATM frauds. It has crossed all the remaining frauds and gives a clear witness on the growing problem in the banking sector due to rising internet usage for banking transactions.

Table 2: Statistics on frauds in banking sector in India

Sl.No.	Type of fraud	Percentage
1	Internet banking and ATM fraud	24%
2	Credit card, debit card frauds	18%
3	Identity fraud	17%
4	Collusion between employees and consumers	15%
5	Funds transfer fraud	13%
6	Bribery and corruption	7%
7	Others	6%

Source: Delloite India Banking Faud Survey, Edition II

c). Strategic Risks

Strategic risks in e-banking are relatively new but it has its implications on the overall performance of e-banking transactions. People with technological, but not banking skills can end up driving the initiatives. E-initiatives can spring up in an incoherent and piecemeal manner in firms. They can be expensive and can fail to recoup their cost. Furthermore, they are often positioned as loss leaders, but may not attract the types of consumers that banks want to expect and may have unexpected implications on existing business lines. Adequacy of management information systems (MIS to track e-banking usage and profitability;

a). Costs involved in monitoring e-banking activities or costs involved in overseeing e-banking activities or costs involved in overseeing e-banking vendors and technology service providers;

b). Design, delivery, and pricing of services adequate to generate sufficient customer demand;

c). Retention of electronic loan agreements and other electronic contracts in a format that will be admissible and enforceable in litigation.

d). Costs and availability of staff to provide technical support for interchanges involving multiple operating systems, web browsers, and communication devices.

A majority of the banks in India offer online and mobile banking services. Most of the transactions are conducted via payment cards, debit and credit cards, and electronic channels such as ATMs. Consequently, both private and public banks as well as other financial institutions in India are becoming increasingly vulnerable to sophisticated cyberattacks. According to RBI, in 2012, 8,322 cases of cyber frauds amounting to 527 million INR were reported. Although the number of cases reported decreased from 15,018 in 2010, the total amount involved increased from 405 in 2012, implying that the average value per cyber fraud case has increased significantly.

d). Security risks

The security risks are posing the tough challenges to the e-banking operations. The transaction security has emerged as the biggest concern among the e-bank's account holders. Transactions risk are creating significant barrier to market acceptance, mismanagement and control are crucial for business reputation and the promotion of consumer confidence as well as operational efficiency.

Many consumers who are doing the online transactons at work place, internet or cyber cafes are becoming the victims of the deceiving of hackers and talented net users (techies). Some of the softwares which have provided the hackers (persons who are having exceptional knowledge in technical usage and expertise in hacking the passwords) to misuse the personal and confidential information used by the online bank account holders. The following particular software programmes provide the hackers benefiting from identifying the Id numbers and passwords of online transactions.

They include:

i.Key Logger

KeyLogger Software allows the users to find out what other users do on a particular computer or laptop in case of absence. Key logger invisibly records keystrokes of every user activity performed on the computer in encrypted log files with option to send the details at specified email id. Best PC monitoring software automatically records all typed emails conversations, chat records, website visited, password and documents lists. This surveillance spy software is extremely easy to use for home and office users. This free version of software which is available in internet is easily downloadable and can be used for a period of 15 days. During this period, any person can install the software and save the secret folder in invisible mode. If a particular user performs e-banking transactions, every key typed by the user will be recorded in a secret folder.

ii. Other Password cracking Softwares

Some of the other important password cracking software tools which will help the people to mis use the online banking transactions are Cain and Abel, John the Ripper,

hash cat, Hydra and ElcomSoft. Many litigation support software packages also include password cracking functionality. Most of the software packages employ a mixture of cracking strategies, with advanced attacks like dictionary attacks, brute force attacks that not only captures the ids and passwords but also provide harm to the entire Personal Computers(PCs) or desktops.

iii. Hacking supported Websites

Apart from the various softwares that are available to easily crack or misuse the information or values of the online bank users there are several hacking supported tools and softwares are provided by the various websites. The use of personal mails, online e-banking ids and passwords can be traced with the instructions available in the various websites. The originality of transaction can be easily misused with the installation of programmes specified in the online hacking supported websites available in net.

iv. Third-Party Dependencies

The partnerships, alliances and outsourcing arrangements with third parties are often becoming complex when the e-banking operations are finding difficult to manage unregulated and un uniformed procedures followed by various banks.

The other risks which are restricting the trustability of e-banking are the financial implications, but from the angle of ease of quantification and the e-banking risk are further classified on the basis of financial risks and Non-financial risks. The financial risks include credit, market, interest rate and liquidity. The non-financial risks include strategic, operational, compliance and reputation risks.

v. OTP by pass

The one time password which the bank provide to the customer's authenticated phone via message and mail is found unsecured. The studies made by the researchers have found that through OTP by pass, the hacker can easily bypass the hurdle of OTP and can transfer the fund with out the two factor authentication in the form of OTP. Eurograbber is the example which has recorded highest frauds in European union.

vi. Cloning

The advent of technology has benefited the hackers in the form of cloning. Due to the consumer unawareness towards the secured usage of authenticated debit/credit cards and mobile sims, the cloning of these became very much rising thus resulting the frauds through duplication of messages occurring to hackers' sims and cards.\

v. Fradulent documentation

Fraudulent documentation involves altering, changing or modifying a document to deceive another person. It can also involve approving incorrect information provided in documents knowingly. Deposit accounts in banks with lax KYC drills/ inoperative accounts are vulnerable to fraudulent documentation. Fraudsters are devising new ways to exploit loopholes in technology systems and processes. In case of frauds involving lower amounts, they employ hostile software programs or malware attacks, phishing, SMSishing and whaling (phishing targeting high net worth individuals) apart from stealing confidential data. In February 2013, the RBI advised banks to introduce certain minimum checks and balances such as the introduction of two factor authentication in case of 'card not present' transactions.

VI. APPROACHES FOR SECURED E-BANKING SERVICES

Mounting operational risks create challenges to the banks and its officials to provide speedy mechanism to settle the risks. The deliberate and active risk control in all aspects right from training the existing employees, use of better technology sources for saving and retrieving information, proper back ups in each block of transactions, taking the assistance of advanced software and software service providers for solving the technical defects and solutions to erroneous transaction processing and failed transactions due to technical difficulty are some of the remedies that are part of risk control system helps in actually reduce operational risks faced by the banks performing e-operations.

The compliance risks are better resolved with the staffing of the experts in bank who are expertise and knowledgeable in strengthening of risk mitigation measures for other related risks and these would reduce legal and compliance risks.

Every bank must develop the risk management frame work that will enable them to face the day to day operational and system risks arise in banking transactions. The expertise help must be taken by the banks in order to prepare good risk management framework for better performance. The information security must be tightened in order to ensure that the consumers will not loss any confidential information to outsiders. The outsourcing management must be planned in order to generate the results that favors the consumers and as well to the bankers. The legal and regulatory barriers can be lessened with the proper utilization of practitioners and making people to participate and share the information to banks about the problems and risk that they face in banking transactions which are conducted through online.

The security problems arise through hacking can be lessened with the proper caring and changing of passwords once in a month or quarterly. The use of virtual key boards enables the users not to get into trap by the softwares including the key board loggers. And, it is to be observed that the misuse of ids and passwords for online transactions are generally occurring when the consumers use the systems or PCs at internet cafes and outside places. Hence, it is suggestable that the banking consumers who use online must use with the PCs which are not under the control of others. The proper

monitoring of programmes installed in the computers and before using the systems, it is suggested that they must restart the PCs and using virtual key boards will make the consumers to come out of the technical loop holes.

It is highly suggestable that the banking personnel must conduct awareness campaigns and 'know your banking' sessions to its consumers in order to make and ensure that the consumers are well aware about the various issues involved in e-banking transaction.

Further, the RBI in collaboration with the banks should adopt the following strategies to counter attack risk issues in e-banking.

a) KYC to KYA

RBI should adopt two eye strategies by enabling KYC to the banks which mainly focuses on identifying, assessing and evaluating the customer as per the documentation submitted by him to avail banking services. Further KYA (Know your accounts) to be adopted to every account holder(i.e., consumer) who avail the services from banks. Lack of awareness is one of the major failures thus leading to frauds. Once in a month/quarterly, every bank owning the consumers should conduct sessions to make aware of the consumer about the secured usage of banking services and awareness on frauds happening in banking network.

b) Strengthening record system

Banks need to maintain multi security record system. Presently the bank is providing the account summary of transfers including receivers bank account number, transaction unique number and date and time of transfer. Banks need to further provide from which IP address/mobile app/mobile number, the transfer is made, recording the receiver's IP address from whether the receiver has checked/downloaded/received the transferred value.

c) Periodic evaluation

Banks should made mandatory to the users to update the account physically once in a month by providing the detailed summary of transactions, mandate change of PIN number, online banking ID, password, transaction password, reverifying the address, mobile number, quality of debit/credit cards being used. This makes the users to have more closeness with banks and they can know exactly about the accounts which they have been using.

VII. CONCLUSIONS AND SUGGESTIONS

E-banking enables higher level of support for consumers in performing their needs. The e-banking has its own limitation and sometimes challenges to the financial security and personal privacy. The study on risk in e-banking is revealing that the benefits of e-banking also provides the problems for users and as well as to the banking personnel in many ways. The compliance, operational and security risks are making the banking personnel to look at the instrument for tightening the issue with proper risk management system. The technical problems are generally deceiving the consumers from the trap of hackers and hence proper caring and attaining the awareness will benefit the consumers and as well as the banking personnel to overcome the problems of e-banking. The periodical surveys, mandate meetings with consumers will enable more closeness among both the parties to have secured transactions to happen in online system.

VIII. REFERENCES:

[1]. Gupta, M., Rao, R., Upadhyaya,S(2004): electronic Banking and Information Assurance Issues: Survey and Synthesis. Journal of Oranizational and End User Computing 16(3), 1, 21 pgs.

[2]. Jayaram Kondabagil (2007), "Risk Management in Electronic Banking – concepts and best practices", John Wiley & Sons Inc., Singapore.

[3]. Liao,S. Chenung, M.T(2003): Challenges to Internet E-banking. Communications of the ACM 46(12), 248=250

[4]. Mahmood Shah & Steve Clarke(2009), "E-Banking Management – Issues, Solutions, and Strategies", Information Science Reference(IGI Global), Hershey PA,USA.

[5]. Ruby Shukla & Pankaj Shukla(2011), "E-banking : Problems and Prospects, IJMBS, Vol.1, Issue1, pp:23-26.

[6]. Sudeep S.(2008), "Internet banking and Customer acceptance: The Indian scenario", Thesis submitted to Cochin University of Science and Technology.

[7]. Xin Chen(2009), "The Challenges and Strategies of Commercial bank in Developing E-banking Business", High Performance Networking, Computing, Communications System, and mathematical Foundations, international Conference Volume, China, pp:68-71.

[8]. http://books.google.co.in/books?id=niDYdutzsnEC&printsec=frontcover&dq=e-banking&hl=en&sa=X&ei=_VAyT4q2D4nUrQev7IWrBA&ved=0CDUQ6AEwAA#v=onepage&q=e-banking&f=false

[9]. http://books.google.co.in/books?id=xoQi4C8mnn0C&pg=PA68&dq=e-banking+risks&hl=en&sa=X&ei=bG0yT-3tHdDhrAe3h5GwBA&ved=0CEoQ6AEwAjgK#v=onepage&q=e-banking%20risks&f=false

[10]. http://www.banktechindia.com/news/11-07-25/Internet_banking_in_India_sees_sevenfold_increase_from_2007.aspx

[11]. ASSOCHAM report on Current fraud trends in the financial sector, June, 2015.

[12]. Deloitte's India Fraud survey, Edition I and EditionII accessed from
[13]. http://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/in-finance-annual-fraud-survey-noexp.pdf and
[14]. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/in-fa-banking-fraud-survey-noexp.pdf

