RISK OF HACKING IN E-BANKING: A STUDY OF PRIVATE SECTOR BANKS

Dr. Sanjeet Kumar
Assistant Professor
Department of Business Administraton
Chaudhary Devi Lal University, Sirsa

Sahila Chaudhry
Research Scholar
Department of Business Administraton
Chaudhary Devi Lal University, Sirsa

Abstract

In the present study, an attempt is made to analyze the risk of hacking in e-banking in the selected private sector banks i.e. AXIS, HDFC and ICICI. A sample of 120 banks' officials (40 from each bank) is taken from the selected banks on the basis of judgement sampling. The primary data were collected with the help of pre-tested structured questionnaire on five point Likert scale i.e. Strongly Agree (SA), Agree (A), Neutral (N), Disagree (D) and Strongly Disagree (SD). For coding and analyzing the data, weights are assigned in order of importance i.e. 1 to Strongly Disagree (SD), 2 to Disagree (D), 3 to Neutral (N), 4 to Agree (A) and 5 to Strongly Agree (SA). The collected data were analyzed through various descriptive and inferential statistical techniques like percentage, mean and standard deviation, etc. Further, ANOVA technique was used to test the hypotheses and validate the results. It is found that easy entry of hackers into the system is ranked as the most significant factor in the selected banks. Further, the disability of significant portion of bank's internal computer system is ranked as the most significant impact in AXIS and ICICI and infringing customers' privacy and its legal implications in HDFC. However, regular review of market place developments is ranked as the most significant measure used in AXIS and ICICI, and proper authorization of end users in HDFC, followed by strategic approach to information security in AXIS, regular review of market place developments in HDFC and sufficient staff with information security expertise in ICICI. It is recommended that password management, firewalls and personal identification number should be used for overcoming the risk of hacking in e-banking in the selected banks. More research should be done on how to integrate the concept of ethics, not just an isolated course but

across the information assurance curriculum. The University administration should consider the issues involved in ethical hacking while designing the information assurance curriculum.

Key Words: Infringing, Authorization, Strategic Approach, Security Expertise

==========

Introduction

Indian banking sector is in the mid of an IT revolution these days. New private sector banks and foreign banks have an edge over public sector banks in the implementation of technological solutions. However, public sector banks are in the process of making huge investment in technology. To be successful in the competitive environment, these banks have to take certain steps like cost reduction by economies of scale, better relations with the customers by providing better services and facilities to them. The changing scenario and the new technologies like internet banking, mobile banking, improvement in payment technology, *etc.* can help in increasing the scale of economies in providing financial services. With the help of technology, banks are now able to offer such products and services, which were difficult or impossible with traditional banking. Indian banks has been able to take one step in this direction - physical cash has been replaced by anytime, anywhere money, but these are more pronounced in foreign and private sector banks. No doubt, e-banking provides so many benefits, but face to face contact between the bank and the customer(s) is absent in e-banking transactions, which causes most of the problems like credit card frauds, fraud of internet, etc. While it mitigates some risks, but induces some risks also. The main risks of e-banking are strategic risk, business risk, operational risk, security risk, privacy/security risk, legal risk, cross-border risk, reputational risk, liquidity risk, etc. These risks are highly interdependent and events that affect one area of risk can have ramifications for a range of other risk categories **(Singh, 2015)**.

Operational risk in e-banking is emerging as a new challenge to the Indian banks, which is a distinct class of risk similar to credit and market risk, and exists in each product and services offered. Examples of operational risk include internal and external fraud, employment practices and workplace safety, clients, products and business practices, damage to physical assets, business disruption and system failures, execution, delivery and process management (for example, data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to

client accounts, non-client counterparty mis-performance, and vendor disputes). Operational risk differs from other banking risks in sense that it is typically not directly taken in return for an expected reward, but exists in the natural course of corporate activity. At the same time, failure to properly manage operational risk can result in a misstatement of an institution's risk profile and expose the institution to significant losses. The objective of operational risk management is the same as for credit and market risks *i.e.* to find out the extent of the financial institution's operational risk exposure, to understand what drives it, to allocate capital against it and identify trends internally and externally that would help in predicting it. Therefore, it should be managed properly so that the technology implementation is smooth and beneficial to the customers and the banking organization. Among the various operational risks, risk of hacking is increasing day by day with the increasing use of technology in providing services to the customers.

Review of Literature

The articles on varied aspects of operational risk in e-banking found in different journals are restrictive in nature and do not give a comprehensive view. *Geiger (2010)* highlighted the renewed interest of banks and the supervisors in operational risk in view of the Basel Committee call for capital charge for operational risk as a component of Pillar I in the new capital adequacy framework of June 1999 and argued that it would be inappropriate to introduce extra capital charge for operational risk in Pillar I. *Trenca and Neag (2010***)** provided an analysis of the operational risk from the perspective of the financial institutions in Romania exposed to operational risk in the context of the Basel II Agreement. The results of the analysis insist on the importance of identifying, measuring and modeling operational risk, and the benefits of continuously improving the instruments, methodology and techniques of operational risk management. *Embrocates and Hofert (2011)* highlighted the introduction of operational risk and summarized the techniques, observed range of practices and supervisory issues in operational risk modeling. He revealed that one of the major problems in operational risk modeling is data scarcity. Without adequate data, this is not possible and therefore still poses challenges to both academia and industry. *Mehra (2011)* explored the range of practices used by Indian banks in management of operational risk essential for achievement of Advanced Measurement Approach (AMA) for a cross-section of Indian

banks and perform a comparative analysis with AMA compliant banks worldwide. The practices of average and small sized public sector bank and old private sector banks were observed to be lagging behind that of new private sector banks regarding the usage of scenarios, updating of these indicators, and collection and usage of external loss data. Wide gap was observed in the range of practices followed by Indian banks and the AMA compliant banks worldwide. *Akbari (2012)* identified, compared and ranked factors affecting operational e-banking risks in viewpoint of customers and employees of Kermanshah Melli bank of Iran. The results indicated that data accuracy, internal controls, technological infrastructure, access to system and security influences the operational risks in e-banking. In the security factors, employees' opinion is more effective than customers, but in case of data accuracy and technological infrastructure, the trend is reversed. *Osunmuyiwa (2013)* examined the various aspects of online banking risks and the methods employed in mitigating these risks and recommended that banks that carry out online banking should clearly explain the privacy rule and communicate to their clients. Banks can also make use of materials like vendor oversight, assignment sheet; excel spreadsheet for risk assessment for policies to carry out data safekeeping. *Singh and Chaudhry (2014)* analyzed the bankers' viewpoint towards various types of e-banking risks in selected public, private and foreign banks in India. The operational risk is found the most important risk in e-banking in all the three categories of banks followed by reputational and legal risk, whereas strategic risk was observed as the least important risk in all the three categories of banks. *Murugavel and Shanthi (2014)* explored the process behind ethical hacking and penetration testing in network security and concluded that ethical hackers use their knowledge and network skills to discover the security vulnerabilities and enlighten the customers, business and secure the system. The foregoing review of literature shows that no concerted effort has been made so far to study the factors responsible for the risk of hacking in e-banking, its impacts on the functioning of the banks and measures to overcome the risk in the selected banks. Therefore, the present study is undertaken to fill the gap in the existing literature.

Scope of Study

The present study is confined to the analysis of risk of hacking in e-banking in selected private sector Indian banks in the area of Punjab, Chandigarh, Haryana, New Delhi and Rajasthan.

Objectives of Study

The present study aims to examine the risk of hacking in e-banking in the selected banks. In this broader framework, the following are the specific objectives of the study:

(i) To identify the factors responsible for risk of hacking in e-banking in the selected banks.

(ii) To examine the impacts of risk of hacking in e-banking on the functioning of the selected banks.

(iii) To analyze the measures to overcome the risk of hacking in e-banking in the selected banks.

Research Hypothesis

The following hypotheses have been formulated and tested to validate the results of the present study:

H_{01}: There is no significant difference among the bankers' viewpoint towards the factors leading to the risk of hacking in e-banking in the selected banks.

H_{02}: There is no significant difference among the bankers' viewpoint towards the impacts of risk of hacking in e-banking on the functioning of the selected banks.

H_{03}: There is no significant difference among the bankers' viewpoint towards the measures for overcoming the risk of hacking in e-banking in selected banks.

Research Methodology

For the purpose of the present study, HDFC Bank (HDFC), ICICI Bank (ICICI) and Axis Bank (AXIS) are selected from the private sector banks. A sample of 120 officials (40 from each bank) is taken from the selected banks on the basis of judgement sampling. The primary data were collected with the help of pre-tested structured questionnaire on five point Likert scale i.e. Strongly Disagree (SD), Disagree (D), Neutral (N), Agree (A), Strongly Agree (SA). For coding and analyzing the data, weights are assigned in order of importance i.e. 1 to Strongly Disagree (SD), 2 to

Disagree (D), 3 to Neutral (N), 4 to Agree (A) and 5 to Strongly Agree (SA). Besides questionnaire, interviews and discussion techniques were also used to unveil the required information. The collected data were analyzed through various descriptive and inferential statistical techniques like percentage, mean, standard deviation, ANOVA technique were used to test the hypotheses and validate the results.

Results and Discussion

Factors Responsible for Risk

As shown in Table 1, easy entry of hackers into the system is ranked as the most significant factor responsible for risk in AXIS (Mean=4.40, SD=1.00) and HDFC (Mean=4.27, SD=0.84) and ICICI (Mean=4.30, SD=0.72), followed by bank's data deliberately corrupted in AXIS (Mean=4.12, SD=1.09) and breach with confidentiality of customers in HDFC (Mean=3.92, SD=0.94) and ICICI (Mean=4.07, SD=0.76). Statistically, ANOVA results show that the respondents in these banks do not differ significantly in their viewpoint towards the factors leading to the risk of hacking in e-banking; therefore the null hypothesis *i.e.* there is no significant difference among the bankers' viewpoint towards the factors leading to the risk of hacking in e-banking in selected banks (H_{01}), is accepted.

Impacts of Risk

As shown in Table 2, disability of significant portion of bank's internal computer system is ranked as the most significant impact in AXIS (Mean=4.20, SD=0.40) and ICICI (Mean=4.25, SD=0.80); and infringing customers' privacy and its legal implications in HDFC (Mean=4.25, SD=0.92), followed by loss of data of accountholders in AXIS (Mean=4.15, SD=1.02) and HDFC (Mean=4.05, SD=1.10); and infringing customers' privacy and its legal implications in ICICI (Mean=4.12, SD=1.01). Statistically, ANOVA results show that the respondents in these banks do not differ significantly in their viewpoint towards the impacts of the risk of hacking in e-banking; therefore the null hypothesis *i.e.* there is no significant difference among the bankers' viewpoint towards the impacts of risk of hacking in e-banking on the functioning of the selected banks (H_{02}), is accepted.

Measures to Overcome the Risk

As shown in Table 3, regular review of market place developments is ranked as the most significant measure in AXIS (Mean=4.40, SD=0.92) and ICICI (Mean=4.47,

SD=0.64); and proper authorization of end users in HDFC (Mean=4.32, SD=0.82), followed by strategic approach to information security in AXIS (Mean=4.05, SD=0.90), regular review of market place developments in HDFC (Mean=4.22, SD=0.94) and sufficient staff with information security expertise in ICICI (Mean=4.40, SD=0.67). Statistically, ANOVA results show that the respondents in these banks differ significantly in their viewpoint towards the sufficient staff with information security expertise (p=0.035) and proper authorization of end users (p=0.044) as measures for overcoming the risk of hacking in e-banking; therefore the null hypothesis *i.e.* there is no significant difference among the bankers' viewpoint towards the measures initiated to overcome the risk of hacking in e-banking in selected banks (H_{03}), is rejected.

Further, the analysis of communication security measures shows that hardware basket tokens is ranked as the most significant measure in AXIS (Mean=4.00, SD=1.13) and HDFC (Mean=4.12, SD=0.88), and password management (Mean=4.40, SD=0.70) in ICICI, followed by employees screening (Mean=4.00, SD=1.24) and firewalls (Mean=3.95, SD=1.01) in AXIS, and firewalls (Mean=4.07, SD=0.91) and personal identification number (Mean=4.05, SD=0.95) in HDFC, and personal identification number (Mean=4.32, SD=0.76) and firewalls (Mean=4.25, SD=0.77) in ICICI. Statistically, ANOVA results show that the respondents in these banks differ significantly towards the password management (p=0.015) as a measure for overcoming the risk of hacking at 5 percent level of significance; therefore the null hypothesis (H_{03}) *i.e.* there is no significant difference among the bankers' viewpoint towards the measures initiated to overcome the risk of hacking in e-banking in selected banks, is rejected.

Conclusion and Policy Implications

As a summary, easy entry of hackers into the system is ranked as the most significant factor leading to the risk of hacking in e-banking in the selected banks. Further, the disability of significant portion of bank's internal computer system is found as the most significant impact in AXIS and ICICI and infringing customers' privacy and its legal implications in HDFC. However, regular review of market place developments is ranked as the most significant measure used in AXIS and ICICI, and proper authorization of end users in HDFC, followed by strategic approach to information security in AXIS, regular review of market place developments in HDFC and sufficient

staff with information security expertise in ICICI. It is recommended that password management, firewalls and personal identification number should be used for overcoming the risk of hacking in e-banking in the selected banks. More research should be done on how to integrate the concept of ethics, not just an isolated course but across the information assurance curriculum. The University administration should consider the issues involved in hacking or ethical hacking while designing the information assurance curriculum.

References

- Akbari P. (2012). A Study of Factors Affecting Operational Electronic Banking Risks in Iran Banking Industry: A Case Study of Kermanshah Melli Bank. International Journal of Management and Business Research, 2 (2), 123-135, spring.
- Embrechts, Paul & Hofert, Marius (2011). Practices and Issues in Operational Risk Modeling under Basel II. Lithuanian Mathematical Journal, 51 (02), April, 180-193.
- Geiger, Hans (2010). Regulating and Supervising Operational Risk for Banks. Presented at the Conference on "Future of Financial Regulation: Global Regulatory Reforms and Implications for Japan" in Tokyo on October 17, accessed on 28.02.2014 from http://www.econbiz.de/archiv1/2008/45350_operational_risk_ banks. pdf
- Mehra, Yogieta S. (2011). Operational Risk Management in Indian Banks: Impact of Ownership and Size on Range of Practices for Implementation of Advanced Measurement Approach. Available at www.igidr.ac.in/conf/money1/operational %20 risk%20management %20in%20Indian%20banks.pdf.
- Murugavel, U. & Shanthi (2014). Survey on Ethical Hacking Process in Network Security. International Journal of Engineering Sciences and Research Technology (IJESRT), 3 (7), July.
- Osunmuyiwa, Olufolabi (2013). Online Banking and the Risks Involved. Research Journal of Information Technology, 5 (2), 50-54.
- Singh, S. & Chaudhry, Sahila (2014). Appraisal of Risks in E-Banking in India. Published in Emerging Paradigm in Management in the Era of Globalization edited

by Ahlawat, Jagbir; Bohra, Monika Tushir, Savera Publishing House, New Delhi, 143-147.

- Singh, S. (2015). Analysis of System Deficiencies in E-Banking. GE - International Journal of Management Research. 3 (7), July, 90-101.
- Trenca, Ioan & Neag, Iulia (2010). Considerations regarding Operational Risk Management in the Context of the Basel II Agreement. The Romanian Economic Journal, 13 (36), 171-186.

Table 1: Factors Responsible for Risk of Hacking in E-banking

Factors	N	AXIS			HDFC			ICICI			ANOVA	
		Mean	S.D.	Rank	Mean	S.D.	Rank	Mean	S.D.	Rank	F	Sig.
Easy entry of hackers into the system	40	4.40	1.00	1	4.27	0.84	1	4.30	0.72	1	0.233	0.793
Breach with confidentiality of customers	40	4.02	0.97	3	3.92	0.94	2	4.07	0.76	2	0.289	0.750
Interference of unauthorized person(s)	40	3.90	1.15	4	3.85	1.16	3	3.92	0.82	3	0.052	0.949
Injecting virus into the system	40	3.45	1.25	6	3.67	1.22	5	3.77	1.12	6	0.764	0.468
Bank's system deliberately crashed	40	3.72	1.33	5	3.65	1.25	6	3.85	1.12	4	0.265	0.768
Bank's data deliberately corrupted	40	4.12	1.09	2	3.72	1.24	4	3.82	1.08	5	1.333	0.268

Source: Survey, **Note:** *= Significant at 5 percent level, Degrees of Freedom (df) =2,117

Table 2: Impacts of Risk of Hacking in E-banking in Selected Banks

Impacts	N	AXIS			HDFC			ICICI			ANOVA	
		Mean	S.D.	Rank	Mean	S.D.	Rank	Mean	S.D.	Rank	F	Sig.
Loss of data of accountholders	40	4.15	1.02	2	4.05	1.10	2	4.10	0.92	3	0.095	0.909
Theft or tempering with customers' information	40	3.80	1.20	5	3.57	1.15	6	3.85	0.97	5	0.691	0.503
Infringing customers' privacy and its legal implications	40	3.97	1.22	3	4.25	0.92	1	4.12	1.01	2	0.668	0.515
Disability of significant portion of bank's internal computer system	40	4.20	0.40	1	4.02	0.83	3	4.25	0.80	1	1.110	0.333
Costs associated with repairing the	40	4.05	1.06	3	4.02	0.97	4	4.05	0.78	4	0.009	0.991

system												
Perceived insecurity of bank's system	40	3.77	1.38	6	3.85	1.16	5	3.82	1.19	6	0.037	0.964

Source: Survey, **Note: ***= Significant at 5 percent level, Degrees of Freedom (df) =2,117

Table 3: Measures to Overcome the Risk of Hacking in E-banking

Measures	N	AXIS			HDFC			ICICI			ANOVA	
		Mean	S.D.	Rank	Mean	S.D.	Rank	Mean	S.D.	Rank	F	Sig.
Regular review of market place developments	40	4.40	0.92	1	4.22	0.94	2	4.47	0.64	1	0.911	0.405
Sufficient staff with information security expertise	40	3.97	1.12	4	3.87	0.99	8	4.40	0.67	2	3.465	0.035*
Penetration testing for vulnerabilities	40	4.02	1.12	3	4.02	1.14	6	4.20	0.82	4	0.378	0.686
Active use of system based security management and monitoring tools	40	3.87	1.18	7	3.87	1.01	9	3.95	1.15	9	0.060	0.942
Surveillance to detect anomalies in usage	40	3.97	0.94	5	4.17	0.81	3	4.15	1.00	7	0.557	0.575
Strong business information security controls	40	3.72	1.28	9	4.05	0.90	5	4.15	0.86	5	1.849	0.162
Strategic approach to information security	40	4.05	0.90	2	4.15	0.76	4	4.20	0.82	3	0.335	0.716
Proper authorization of end users	40	3.77	1.18	8	4.32	0.82	1	4.15	0.92	6	3.217	0.044*
Building security control best practices into the system and network	40	3.92	0.91	6	3.92	1.04	7	4.02	0.99	8	0.136	0.873
Development of Communication Security Measures:												
Firewalls	40	3.95	1.01	3	4.07	0.91	2	4.25	0.77	3	1.105	0.335
Password management	40	3.82	1.21	8	3.77	1.16	8	4.40	0.70	1	4.331	0.015*
Encryption techniques	40	3.95	1.28	5	3.57	1.23	10	4.20	0.91	5	2.967	0.055
Collaborating websites	40	3.95	1.28	6	3.75	1.17	9	3.97	1.16	9	0.418	0.660
Authentication	40	3.82	1.17	7	4.05	0.95	4	4.05	1.08	8	0.583	0.560
Personal Identification Number	40	3.97	1.16	4	4.05	0.95	3	4.32	0.76	2	1.423	0.245
Hardware basket tokens	40	4.00	1.13	1	4.12	0.88	1	3.92	0.99	10	0.401	0.671
Virus controls	40	3.82	1.33	9	3.95	0.95	6	4.20	1.04	6	1.152	0.319

Biometrics	40	3.80	1.28	10	4.00	1.10	5	4.20	0.91	4	1.293	0.278
Employees screening	40	4.00	1.24	2	3.82	1.29	7	4.10	0.98	7	0.555	0.576
Encryption techniques	40	3.95	1.28	5	3.57	1.23	10	4.20	0.91	5	2.967	0.055
Collaborating websites	40	3.95	1.28	6	3.75	1.17	9	3.97	1.16	9	0.418	0.660

Source: Survey, **Note: ***=Significant at 5 percent level, Degrees of Freedom (df) =2,117