International Journal of Marketing and Management Research
Vol. 8, Issue 4, April 2017, Impact Factor; 5.108 ISSN: (2229-6883)
www.skirec.org Email Id: skirec.org@gmail.com

RISK OF INADEQUATE CUSTOMERS' SECURITY PRACTICES IN INDIAN BANKS

Dr. Sahila Chaudhry

Research Scholar, Department of Business Administration,

Chaudhary Devi Lal University, Sirsa,

Haryana, India

ABSTRACT

In the present study, an attempt is made to analyze the group-wise bankers' viewpoint towards the risk of inadequate customers' security practices in public and private sector Indian banks. A sample of 440 banks' officials is taken on the basis of judgement sampling i.e. 120 from State Bank Group, 200 from Nationalized Banks and 120 from Private Sector Banks. 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). 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 lack of awareness about the compliance of security mechanism and lack of reliability of information system are the main factors responsible for the risk of inadequate customers' security practices in the selected banks. Further, financial loss through unauthorized transactions and potential adverse publicity about the bank are the significant impacts on the functioning of the risk on these banks. However, providing information to the customers on the importance of safeguarding information in non-secure transactions and incorporating security measures into products and services are most adopted measures for overcoming the risk of inadequate customers' security practices in the selected groups of banks. It is recommended that banks should implement reasonable measures to assess and enforce compliance with the established policies and procedures, and enforce rules requiring strong, hard guessing user IDs, and passwords.

KEYWORDS: *Security, Electronic, Safeguarding, Transactions, Unauthorized*

INTRODUCTION

Indian banks are in the process of implementation of technological solutions these days. But public sector banks are far behind in this process, therefore there is a huge scope for automation in these banks *(www.centralbank.ie)*. No doubt, technology has been helpful for enhancing the customers' convenience in the products and services offered, which were difficult earlier with traditional banking. But the security of the transactions is a major concern in the use of technology as it induces some risks which are highly interdependent and events that affect one area of risk can also have ramifications for a range of other risk categories *(Singh, 2015).* Among these risks, operational risk is emerging as a new challenge to the Indian banks, which exists in each product and services offered and is not directly taken in return for an expected reward. The failure in properly managing the operational risk can result in a mis-statement of an institution's risk profile and expose the institution to significant losses *(www.fsrc.gov.ag)*. Operational risk is confronted by the bank even before it decides its first credit transaction realizing that the merely a quantitative approach to credit risk and market risk overlooks the key danger areas and that operational risk management should consequently be developed into a discipline *(Geiger, 2000).*The regulatory authorities have also renewed their interest in operational risk as they feel that about 25 percent of regulatory capital is needed for operational risk *(Akbari, 2012)*. Increasing dependence on computers and electronic communication in banking transactions has increased the possibility of system failure, which adversely affects its business. Risk of inadequate customers' security practices, which is an important component of operational risk, is the risk arising due to failure of the bank in maintaining the confidentiality of information of the customers' account, which results in breach of faith and migration of customers to other competing banks.

REVIEW OF LITERATURE

The articles on different aspects of operational risk are restrictive in nature and do not give a comprehensive picture. *Adrian (1999)* examined the optimal relationship between operational risk and reward; and concluded that a systematic approach to manage operational risk will be more effective and efficient than allowing an informal and intuitive process to operate. *Sood (2004)* examined the factors responsible for operational risk, present practices on quantification of operational risk, sound practices and governing principles of operational risk management; and recommended that it would be

appropriate for Indian banks to strengthen their MIS system, retain/re-skill the staff and put in place the comprehensive risk management policy. *Jobst (2007)* stated that with the increased size and complexity of the banking industry, operational risk has a greater potential to transpire in more harmful ways than many other sources of risk. The current regulatory framework of operational risk under the New Basel Capital Accord was overviewed with a view to inform a critical debate about the influence of varying loss profiles and different methods of data collection, loss reporting and model specification on the reliability of operational risk estimates and the consistency of risk-sensitive capital rules. *Jankiraman (2008)* assessed the status of operational risk management in the Indian banking system in the context of Basel II and the approach adopted for computation of capital required for operational risk is compared broadly with the banking system in Asia, Africa and Middle East. A survey on 22 Indian banks was conducted, which indicated the need to devote more time and resources if the banks desire to implement the advanced approaches under Basel *Jian et al. (2009)* examined the influence of capital structure and operational risk on profitability of the life insurance industry in Taiwan. The results show that the profitability decreased with the higher debt-equity ratio; hence the regulatory organizations must urge insurance companies to effectively diversify their investments and employ risk avoidance strategies. Effective use of hedging and diversifying will also help to divide risk and create financial revenue. *Tanase and Serbu (2010)* said that the operational risk is generated primarily as a result of direct customer interaction with the credit institution. But the provision of e-banking services reduced direct contact with banks' customers and thus reduced potential losses arising from operational risk. They considered it necessary to be aware of the relationship between operational risks and e-banking services promoted by the banks and of the importance of this connection especially in a financial environment affected by the financial crisis. *Embrechts and Hofert (2011)* summarized the techniques, observed range of practices and supervisory issues in operational risk modeling, and found that one of the largest problems in operational risk modeling is data scarcity, therefore poses the challenges to both academia and industry. *Akbari (2012)* identified, compared and ranked the factors affecting operational risk in e-banking from the viewpoints 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 risk in e-banking in the selected bank. In the security factors,

employees' opinion is more effective than customers, but in case of data accuracy and technological infrastructure, the trend is reversed. *Singh and Chaudhry (2014)* analyzed the bankers' viewpoint towards various types of e-banking risks in selected public, private and foreign banks in India and operational risk is found as the most important risk in e-banking in all the three categories of banks, followed by reputational and legal risk. Further, the difference in the bankers' viewpoint towards various types of risks in e-banking is also found significant. *Epetimehin and Fatoki (2015)* examined the regulatory framework related to operational risk management with a sample of 150 employees from different financial institutions such as banks, insurance, stock brokers and microfinance companies. The results showed that operational risk management has positive effects on the financial development and growth in the financial sector. The foregoing review of literature shows that no concerted effort has been made to examine the risk of inadequate customers' security practices in e-banking scenario, therefore the present study is undertaken to fill the gap in the existing literature.

SCOPE OF THE STUDY

The present study is conducted to examine the bankers' viewpoint towards the risk of inadequate customers' security practices in the selected banks located in the area of Punjab, Chandigarh, Haryana, New Delhi and Rajasthan in India.

RESEARCH OBJECTIVES

The following are the specific objectives of the study:

(i) To identify the factors responsible for risk of inadequate customers' security practices in the selected banks.

(ii) To examine the potential impacts of risk of inadequate customers' security practices on the functioning of the selected banks.

(iii) To analyze the measures to overcome the risk of inadequate customers' security practices in the selected banks.

RESEARCH HYPOTHESES

The following research 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 responsible for risk of inadequate customers' security practices in the selected groups of banks.

H_{02}: There is no significant difference among the bankers' viewpoint towards the potential impacts of risk of inadequate customers' security practices on the functioning of the selected groups of banks.

H_{03}: There is no significant difference among the bankers' viewpoint towards the measures for overcoming the risk of inadequate customers' security practices in the selected groups of banks.

RESEARCH METHODOLOGY

SAMPLE PROFILE

The population for the present study is the Indian banking sector, which is divided into three categories *i.e.* State Bank Group, Nationalized Banks and Private Sector Banks. State Bank of India (SBI), State Bank of Patiala (SBOP), State Bank of Bikaner and Jaipur (SBBJ) from the category of State Bank group; Punjab National Bank (PNB), Dena Bank (DENA), Oriental Bank of Commerce (OBC), Andhra Bank (ANDRA), and Syndicate Bank (SYNDI) from the category of nationalized banks; and HDFC Bank (HDFC), ICICI Bank (ICICI) and Axis Bank (AXIS) from the category of private sector banks are selected for the present study. A sample of 440 banks officials (40 from each bank) is taken on the basis of judgement sampling. Out of 440 respondents, 99 respondents (22.5 percent) are having the experience of less than four years, 140 respondents (31.8 percent) are having the experience of 5-8 years and 201 respondents (45.7 percent) are having the experience of more than 8 years. On the other hand, 317 respondents (72 percent) are postgraduates, 121 respondents (27.5 percent) are graduates and 02 (0.50 percent) are having professional qualification like CA, CS, *etc.*

DATA COLLECTION

The present study is of exploratory-cum-descriptive in nature. Accordingly both types of data *i.e.* primary and secondary were used. 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) and Strongly Agree (SA) from the bank officials of branches of the selected located in the areas of Delhi, Rajasthan, Haryana, Chandigarh and Punjab. On the other hand, secondary data were collected

from journals, magazines, websites, reports of RBI and IBA, *etc.* Besides questionnaire, interviews and discussion techniques were also used to unveil the required information.

DATA ANALYSIS

The collected data were analyzed through various descriptive and inferential statistical techniques like frequency distribution, percentage, mean, standard deviation, *etc.* with the help of SPSS (18.0 version). For coding and editing the data, weights were 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). Further, ANOVA (one-way) technique was used to test the research hypotheses and validate the results of the study. The reliability of the scale used for collection of data is evaluated by calculating the value of Cronbach alpha coefficient, which is 0.771 at 5 percent level of significance, so the scale is considered reliable.

RESULTS AND DISCUSSIONS

FACTORS RESPONSIBLE FOR RISK

As displayed in Table 1 (A), lack of awareness about the compliance of security mechanism in State Bank Group (Mean=4.10, SD=0.89) and lack of reliability of information system in Nationalized Banks (Mean=4.09, SD=1.05) and Private Sector Banks (Mean=4.22, SD=0.95), followed by lack of reliability of information system in State Bank Group (Mean=3.95, SD=1.19) and lack of awareness about the compliance of security mechanism in Nationalized Banks (Mean=4.01, SD=0.0.91) and Private Sector Banks (Mean=3.90, SD=1.02). The mean score of all the statements, which is greater than 3.00, implies that most of the respondents agree with the factors responsible for risk of inadequate customers' security practices in the selected groups of banks. Statistically, ANOVA results show that the respondents in the selected groups of banks do not differ significantly towards the factors responsible for risk of inadequate customers' security practices at 5 percent level of significance; therefore the null hypothesis (H_{01}) is accepted. Further, the results of Post-hoc analysis (multiple comparisons) also show that there is no significant difference in the respondents' viewpoint of the selected groups of banks towards the factors responsible for the risk of inadequate customers' security practices at 5 percent level of significance.

As revealed from Table 1 (B)**,** taking all the selected eleven banks together, lack of reliability of information system (Mean=4.09, SD=1.07) is ranked as the top most factor responsible for risk of

inadequate customers' security practices, followed by lack of awareness about the compliance of security mechanism (Mean=4.00, SD=0.94) and use of personal information by the customers in non-secure electronic transactions (Mean=3.82, SD=1.13). The mean score of all the statements, which is greater than 3.00, implies that most of the respondents agree with the factors responsible for the risk of inadequate customers' security practices in the selected banks. Statistically, ANOVA results show that the respondents in the selected banks do not differ significantly towards the factors responsible for the risk of inadequate customers' security practices at 5 percent level of significance; therefore the null hypothesis (H_{01}) is accepted.

IMPACTS OF RISK

As displayed in Table 2 (A), financial loss through unauthorized transactions is ranked as the significant impact in State Bank Group (Mean=4.05, SD=1.03), Nationalized Banks (Mean=4.16, SD=0.86) and Private Sector Banks (Mean=4.25, SD=0.95), followed by potential adverse publicity about the bank in State Bank Group (Mean=4.00, SD=1.11) and Private Sector Banks (Mean=4.00, SD=0.95), and loss of existing and potential customers in Nationalized Banks (Mean=3.98, SD=0.97). The mean score of all the statements, which is greater than 3.00, implies that most of the respondents agree with the impacts of risk of inadequate customers' security practices on the functioning of the selected groups of banks. Statistically, ANOVA results show that the respondents in the selected groups of banks do not differ significantly towards the impacts of risk of inadequate customers' security practices on the functioning of the selected banks at 5 percent level of significance; therefore the null hypothesis (H_{02}) is accepted. Further, the results of Post-hoc analysis (multiple comparisons) also show that there is no significant difference in the respondents' viewpoint of the selected groups of banks towards the impacts of the risk of inadequate customers' security practices at 5 percent level of significance.

As revealed from Table 2 (B), taking all the selected banks together, financial loss through unauthorized transactions (Mean=4.16, SD=0.93) is ranked as the most significant impact of the risk of inadequate customers' security practices on the functioning of the selected banks, followed by loss of existing and potential customers (Mean=3.96, SD=1.07). The mean score of all the statements, which is greater than 3.00, implies that most of the respondents agree with the impacts of risk of inadequate customers' security practices on the functioning of the selected banks. Statistically, ANOVA results show that the

respondents in the selected banks do not differ significantly towards the impacts of the risk of inadequate customers' security practices on the functioning of the selected banks at 5 percent level of significance; therefore the null hypothesis (H_{02}) is accepted.

MEASURES FOR OVERCOMING THE RISK

As displayed in Table 3 (A), providing information to the customers on the importance of safeguarding information in non-secure transactions is ranked at the top in State Bank Group (Mean=4.38, SD=0.80), Nationalized Banks (Mean=4.28, SD=0.87), Private Sector Banks (Mean=4.34, SD=0.78), followed by incorporating security measures into products and services in State Bank Group (Mean=4.26, SD=0.81), Nationalized Banks (Mean=4.00, SD=0.97) and Private Sector Banks (Mean=4.10, SD=0.90). The mean score of all the statements, which is greater than 3.00, implies that most of the respondents agree with the measures for overcoming the risk of inadequate customers' security practices in the selected groups of banks. Statistically, ANOVA results show that the respondents in the selected groups of banks differ significantly towards incorporating security measures into products and services (p=0.048) as a measure for overcoming the risk of inadequate customers' security practices at 5 percent level of significance; therefore the null hypothesis (H_{03}) is rejected. Further, the results of Post-hoc analysis (multiple comparisons) also show that there is a significant difference in the respondents' viewpoint of State Bank Group and Nationalized Banks towards incorporating security measures into products and services (p=0.037) as a measure for overcoming the risk of inadequate customers' security practices at 5 percent level of significance.

As revealed from Table 3 (B)**,** taking all the selected eleven banks together, providing information to the customers on the importance of safeguarding information in non-secure transactions (Mean=4.32, SD=0.83) is ranked as the most significant measure for overcoming the risk of inadequate customers' security practices, followed by incorporating security measures into products and services (Mean=4.10, SD=0.92), ensuring that the necessary level of secrecy is enforced at each stage of data processing and prevents unauthorized disclosure (Mean=4.02, SD=1.06), addressing specific security issues that management feels need more detailed explanation (Mean=4.01, SD=1.02) and making sure that a comprehensive structure is built and all employees understand how they have to comply with these security issues (Mean=3.98, SD=1.06). The mean score of all the statements, which is greater than 3.00,

implies that most of the respondents agree with the measures for overcoming the risk of inadequate customers' security practices in the selected banks. Statistically, ANOVA results show that the respondents in the selected banks differ significantly towards incorporating security measures into products and services (p=0.005) as a measure for overcoming the risk of inadequate customers' security practices at 5 percent level of significance; therefore the null hypothesis (H_{03}) is rejected.

CONCLUSIONS AND RECOMMENDATIONS

To sum up, lack of awareness about the compliance of security mechanism and lack of reliability of information system are the main factors responsible for the risk of inadequate customers' security practices in the selected banks. Further, financial loss through unauthorized transactions and potential adverse publicity about the banks are the significant impacts of the risk on the functioning on these banks. However, providing information to the customers on the importance of safeguarding information in non-secure transactions and incorporating security measures into products and services are most adopted measures for overcoming the risk of inadequate customers' security practices in the selected groups of banks. It is recommended that banks should implement reasonable measures to assess and enforce compliance with the established policies and procedures, and enforce rules requiring strong, hard to guess user IDs, and passwords. Customers should also be made aware about the information security as 100 percent security guarantee for users' transactions is possible only if both the banks and customers together give flawless security posture to online banking. There should be a well-documented incident management process to handle security incidents and all the end users must be aware of the process. The process should clearly spells out the responsibilities and steps for orderly response to a security incident.

REFERENCES

Adrian, Sparrow (1999). A Theoretical Framework for Operational Risk Management and Opportunity Realization. Treasury Working Paper 00/10, accessed on 28.02.2014 from www.treasury.govt.nz/publications/research-policy/wp/.../twp 00-10. pdf

Akbari, P. (2012). A Study on Factors Affecting Operational Electronic Banking Risks in Iran Banking Industry. *International Journal Management Business Research*: *Spring*, 2 (2), 123-135 https://www.ccg-catalyst.com/bank-consulting/bank-operational-risk

Embrechts, Paul & Hofert, Marius (2011). Practices and Issues in Operational Risk Modeling under Basel II. *Lithuanian Mathematical Journal,* 51 (02), April, 180-193.

Epetimehin, F. M. and Fatoki, O. (2015). Operational Risk Management and the Financial Sector Development: An Overview. *International Journal of Economics, Commerce and Management*, 3 (3), 1-11.

Jankiraman, Usha (2008). Operational Risk Management in Indian Banks in the context of Basel II: A Survey of the State of Preparedness and Challenges in Developing the Framework. *Asia Pacific Journal of Finance and Banking Research,* 2 (2), 26-44

Jian, Shen Chen; Mei-Ching, Chen; Wen-Ju, Liao & Tsung-Hsien, Chen (2009). Influence of Capital Structure and Operational Risk on Profitability of Life Insurance Industry in Taiwan. *Journal of Modelling in Management,* 4 (1), 7-18

Jobst, Andreas A. (2007). Consistent Quantitative Operational Risk Measurement and Regulation: Challenges of Model Specification, Data Collection and Loss Reporting. IMF Working Papers, 1-46, November, available at http://ssrn.com/abstract= 1087169.

Singh, S. & Chaudhry, Sahila (2014). Appraisal of Risks in E-Banking in India. Published in Emerging Paradigms in Management in the Era of Globalization edited by Ahlawat, Jagbir; Bohra and 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

Sood, Rajesh Kumar (2004). Operational Risk under New Basel Accord. *IBA Bulletin,* XXVI (06), June, 21-29.

Tanase, R. D. and Serbu R. (2010). Operational Risk and E-banking. *Bulletin of the Transivania University of Brasov*, Series V, Economic Sciences, 3 (1), 327-334.

Other Related Links

www.centralbank.ie

www.fsrc.gov.ag

International Journal of Marketing and Management Research
Vol. 8, Issue 4, April 2017, Impact Factor; 5.108 ISSN: (2229-6883)
www.skirec.org Email Id: skirec.org@gmail.com

Table 1 (A): Factors Responsible for Risk of Inadequate Customers' Security Practices in Selected Groups of Banks

Factors	State Bank Group				Nationalized Banks				Private Sector Banks				ANOVA	
	N	Mean	S.D.	Rank	N	Mean	S.D.	Rank	N	Mean	S.D.	Rank	F	Sig.
Lack of reliability of information system	120	3.95	1.19	2	200	4.09	1.05	1	120	4.22	0.95	1	1.857	0.157
Lack of awareness about the compliance of security mechanism	120	4.10	0.89	1	200	4.01	0.91	2	120	3.90	1.02	2	1.247	0.288
Use of personal information by the customers (credit card numbers, bank account numbers) in non-secure electronic transmissions	120	3.81	1.25	3	200	3.79	1.10	3	120	3.90	1.06	3	0.331	0.718
Access of confidential information of customers accounts by criminals	120	3.73	1.17	4	200	3.77	1.14	4	120	3.77	1.22	4	0.048	0.954

Source: Survey, **Note:** *= Significant at 5 percent level, Degrees of Freedom (df) = 2,437.

Table 1 (B): Factors Responsible for Risk of Inadequate Customers' Security Practices in the Selected Banks

Factors	N/P	Response						Descriptive Statistics			ANOVA	
		SD	D	N	A	SA	Total	Mean	S.D.	Rank	F	Sig.
Lack of reliability of information system	N	16	42	13	184	185	440	4.09	1.07	1	1.401	0.177
	P	3.6	9.5	3.0	41.8	42.0	100.0					
Lack of awareness about the compliance of security mechanism	N	11	34	25	241	129	440	4.00	0.94	2	0.890	0.543
	P	2.5	7.7	5.7	54.8	29.3	100.0					
Customer use of personal information (credit card numbers, bank account numbers) in non-secure electronic transmissions	N	20	58	32	197	133	440	3.82	1.13	3	1.356	0.198
	P	4.5	13.2	7.3	44.8	30.2	100.0					
Access of confidential information of customers accounts by criminals	N	29	55	28	208	120	440	3.76	1.17	4	0.956	0.481
	P	6.6	12.5	6.4	47.3	27.3	100.0					

Source: Survey, **N**=Number of Respondents, **P**=Percent, Degree of Freedom (df)=10,429, *=Significant at 5 percent level.

International Journal of Marketing and Management Research
Vol. 8, Issue 4, April 2017, Impact Factor; 5.108 ISSN: (2229-6883)
www.skirec.org Email Id: skirec.org@gmail.com

Table 2 (A): Impacts of Risk of Inadequate Customers' Security Practices in Selected Groups of Banks

Impacts	State Bank Group				Nationalized Banks				Private Sector Banks				ANOVA	
	N	Mean	S.D.	Rank	N	Mean	S.D.	Rank	N	Mean	S.D.	Rank	F	Sig.
Financial loss through unauthorized transactions	120	4.05	1.03	1	200	4.16	0.86	1	120	4.25	0.95	1	1.266	0.283
Potential adverse publicity about the bank	120	4.00	1.11	2	200	3.89	1.01	3	120	4.00	0.95	2	0.679	0.507
Loss of existing and potential customers	120	3.95	1.19	3	200	3.98	0.97	2	120	3.92	1.12	3	0.121	0.886

Source: Survey, **Note:** *= Significant at 5 percent level, Degrees of Freedom (df) = 2,437

Table 2 (B): Impacts of Risk of Inadequate Customers' Security Practices in Selected Banks

Impacts	N/P	Response						Descriptive Statistics			ANOVA	
		SD	D	N	A	SA	Total	Mean	SD	Rank	F	Sig.
Financial loss through unauthorized transactions	N	10	28	19	208	175	440	4.16	0.93	1	1.591	0.106
	P	2.3	6.4	4.3	47.3	39.8	100.0					
Potential adverse publicity about the bank	N	14	42	31	217	136	440	3.95	1.02	3	0.464	0.913
	P	3.2	9.5	7.0	49.3	30.9	100.0					
Loss of existing and potential customers	N	15	49	28	195	153	440	3.96	1.07	2	1.436	0.161
	P	3.4	11.1	6.4	44.3	34.8	100.0					

Source: Survey, **N**=Number of Respondents, **P**=Percent, Degree of Freedom (df)=10,429, *=Significant at 5 percent level

Table 3 (A): Measures for Overcoming the Risk of Inadequate Customers' Security Practices in Selected Groups of Banks

Measures	State Bank Group				Nationalized Banks				Private Sector Banks				ANOVA	
	N	Mean	S.D.	Rank	N	Mean	S.D.	Rank	N	Mean	S.D.	Rank	F	Sig.
Providing information to the customers on the importance of safeguarding information in non-secure transactions	120	4.38	0.80	1	200	4.28	0.87	1	120	4.34	0.78	1	0.549	0.578
Incorporating security measures into products and services	120	4.26	0.81	2	200	4.00	0.97	2	120	4.10	0.90	2	3.056	0.048*
Enforcing necessary level of secrecy at each stage of data processing and prevents unauthorized disclosure	120	4.14	1.09	3	200	3.94	1.11	6	120	4.03	0.94	3	1.351	0.260
Providing directions for all future security activities within the organization	120	3.92	1.06	7	200	3.97	1.08	4	120	4.01	1.01	4	0.225	0.799

International Journal of Marketing and Management Research
Vol. 8, Issue 4, April 2017, Impact Factor; 5.108 ISSN: (2229-6883)
www.skirec.org Email Id: skirec.org@gmail.com

Addressing specific security issues that management feels more detailed explanation	120	4.10	1.06	5	200	3.99	1.04	3	120	3.98	0.97	5	0.523	0.593
Building a comprehensive structure and ensuring that all employees understand how they have to comply with these security issues	120	4.09	1.04	6	200	3.96	1.05	5	120	3.93	1.11	6	0.790	0.454
Presenting the management's decisions that are specific to the actual computers, networks, applications and data	120	4.12	1.04	4	200	3.92	1.11	7	120	3.88	1.16	7	1.730	0.179

Source: Survey, **Note:** *= Significant at 5 percent level, Degrees of Freedom (df) = 2,437

Table 3 (B): Measures for Overcoming the Risk of Inadequate Customers' Security Practices in the Selected Banks

Measures	N/P	Response						Descriptive Statistics			ANOVA	
		SD	D	N	A	SA	Total	Mean	SD	Rank	F	Sig.
Provide information to the customers on the importance of safeguarding information in non-secure transactions.	N	9	13	10	201	207	440	4.32	0.83	1	1.003	0.439
	P	2.0	3.0	2.3	45.7	47.0	100.0					
Incorporate security measures into products and services	N	9	34	10	237	150	440	4.10	0.92	2	2.554	0.005*
	P	2.0	7.7	2.3	53.9	34.1	100.0					
Ensures that the necessary level of secrecy is enforced at each stage of data processing and prevents unauthorized disclosure	N	19	38	18	205	160	440	4.02	1.06	3	1.737	0.070
	P	4.3	8.6	4.1	46.6	36.4	100.0					
Provide scope and direction for all future security activities within the organization	N	16	47	15	218	144	440	3.97	1.05	6	1.278	0.240
	P	3.6	10.7	3.4	49.5	32.7	100.0					
Address specific security issues that management feels need more detailed explanation	N	12	46	18	210	154	440	4.01	1.02	4	0.397	0.948
	P	2.7	10.5	4.1	47.7	35.0	100.0					
Make sure that a comprehensive structure is built and all employees understand how they have to comply with these security issues	N	17	45	16	210	152	440	3.98	1.06	5	1.312	0.221
	P	3.9	10.2	3.6	47.7	34.5	100.0					
Present the management's decisions that are specific to the actual computers, networks, applications and data	N	25	38	16	209	152	440	3.96	1.11	7	1.786	0.061
	P	5.7	8.6	3.6	47.5	34.5	100.0					

Source: Survey, **N**=Number of Respondents, **P**=Percent, Degree of Freedom (df)=10,429, *=Significant at 5 percent level.