Information Security Management Practices of Indian Banks

Venkatachalam.S[1] Padmaavathy.PA[2] Priya Elizabeth Issac [3]

ABSTRACT

The dawn of technology and internet enabled banking products and services has obtained many information securities related concerns to the banking and financial organizations. As banking organizations deal with people's money, they are accountable for safeguarding the privacy and the integrity of customer information. Therefore, banks need to ensure that the information security management practices are strictly followed to avoid information security incidents. This study is to understand the information security management practices followed by the Indian banks.

Key Words: *Information security, banking, information security practices, information security policy.*

1. INTRODUCTION

Banking and financial services have a significant role in a country's economic development. The advent of technology and internet enabled services brought in new products and services to the customers. Internet enabled services brought banking at doorsteps and at a faster pace. When banking becomes more exposed and convenient to its customers, it has also brought in equal number of vulnerabilities. Banks are obliged to maintain the integrity of banking transactions and safeguarding the privacy of its customers. Hence, information security management practices have great relevance in today's scenario. The present study is an attempt to understand the information security management practices of Indian banks.

2. REVIEW OF LITERATURE

Information and information assets are very important to service organizations and especially banking organizations. As banking deals with large volume of customer data, protection to information and information assets is of paramount importance. While the latest technology adoptions and internet banking increased the pace in banking services and add more convenience to customers, it has opened room for more vulnerabilities (Ambhire & Teltumde, 2011). The major concerns are of security and privacy of information (Brar et al., 2012). Protecting the security of information assets is a common concern among the civilized and developing countries (Farn et al., 2004). A sound security system is required for the development, implementation and maintenance of internet banking (Hutchinson & Warren, 2003). Information security principles and practices are placed in both prevention and response paradigms. While in prevention paradigm it manages the predicted threats, in response paradigm it manages the unpredicted or unforeseen threats (Baskerville et al., 2014). The implementation of information security management is a strategic decision and are determined by the organization's needs and objectives, process and

[1] Associate Professor, Depart of Management, Karpagam Academy of Higher Education, Coimbatore, India. Researcher ID: B-1662-2019. Scopus Author ID: 57205545948.
[2] Assistant Professor, Depart of Management, Karpagam Academy of Higher Education, Coimbatore, India
[3] P.hD Research Scholar, Depart of Management, Karpagam Academy of Higher Education, Coimbatore, India

procedures, size and structure, and the security requirements (Salgovicova & Prajova, 2012). For an effective information security management, efficient security resources are to be deployed at various levels- attacks prevention, vulnerability reduction and threat identification (Nazareth & Choi, 2015). However, the current tools used for assessing information security threats were not integrated to the organization's information security policy. The information security policy can act as a guide to protect and manage all critical assets, people and infrastructure (Mbowe et al., 2014)

Many IT related functions of banking and financial industry are outsourced. So, banks need to take proactive steps against all possible information security threats (Podebrad & Drotleff (2009). Fenz et al. (2014) stated that as the technology advances, there are several challenges to information security managers to frame a sound information security system. An effective information security management system can reduce the possible risks or threats in an organization (Wawak, 2010). According to the study conducted by Ma et al. (2008), more awareness on information security aspects should be provided by information security professionals to management and employees; and management should also give top priority to information security management and an experienced person should be made in charge of information security management to have a good information security management practice in the organization. For effective risk management, information security standards must be implemented at all levels of the organization. The information security management is an on-going process of risk assessment which includes identifying the possible risks or threats, possible tolerance level, setting up of controls and executing plans to address the identified risks or threats (Yildirim, 2016).

International information security management guidelines have a significant role in managing and certifying the information security practices of organizations. These set of standards ensure that the best security practices are implemented and an acceptable level of security is attained. There exist several standards on information security like ISO 27001, PCI-DSS and COBIT and each has its own role and position in the information security management system (Alber & Nabil, 2015). However, these information security guidelines are generic in nature, hence organizations need to have a tailor-made approach while implementing information security management practices (Siponen & Willison, 2009). Since people are the weakest link in the information security management system, behavioural aspects of information security also have great relevance (Gonzalez & Sawicka, 2002; Mishra et al., 2006). Hence, while implementing and maintaining information security system the information security policies and practices and the people responsible for handling information security management must be given high importance.

3. RESEARCH METHODOLOGY

Research Objectives

- To understand the information security practices followed by the Indian banks.
- To evaluate the information security practices followed by the public and private sector banks in Kerala.
- To provide suggestions based on the outcome of the study.

Scope of the study

The banking industry in India has achieved great heights in all these years. Indian banking industry boasts of having banking practices from traditional to modern, from nationalization to privatization with increasing number of foreign banks in India. The adoption of technology brought a revolution to the industry with varied products and services. However, the changing banking business has brought in equal number of risks to banking. Hence the banking organizations must follow information security practices to protect their data and information. The study is to analyse the information security practices followed by the banks in Kerala, India.

Research Design

The study was conducted among the banks headquartered in Kerala by using census method. The data has been collected through a structured questionnaire with Likert scale method (Stewart & Jurjens,2017). As the study was technical in nature, it was collected from IT employees who were responsible for information security management of both public and private sector banks headquartered in Kerala.

4. ANALYSIS & INTERPRETATION

The following analysis and interpretations show the perception of Information Security Practices among the employees of responding banks.

Table 4.1 Mean (percentage score) for each statement related to information security practices for the respondents of each bank

Sl. No.	Statements	Total
QA1	In our bank, top management give high regards to information security	3.65 (91.22)
QA2	In our bank, there exists regular review on information security policy	3.44 (86.01)
QA3	In our bank, there exist a documented information security policy	3.63 (90.63)
QA4	In our bank, roles and responsibilities of employees are clearly defined in information security policy	3.22 (80.51)
QA5	In our bank, employees are aware of information security policies and guidelines	2.49 (62.35)
QA6	In our bank, regular training programmes on information security are conducted	2.50 (62.5)
QA7	In our bank, there exist regular risk assessment and risk management practices	3.37 (84.23)
QA8	There exists documented recovery and business continuity plan	3.46 (86.46)

From the table 4.1, it was observed that “top management gives high regard to information security” and “existence of documented information security policy” ranks the top. It was also observed that “employees’ awareness of information security policy” and “conducting regular training programmes on information security” scored the last position.

Table 4.2 Comparison the response [Mean (percentage score)] for each statement related to information security practices among the respondents of private sector and public sector banks

Sl. No.	Statements	Private	Public	Total	Z-value	p-value
QA1	In our bank, top management give high regards to information security	3.69 (92.25)	3.52 (88)	3.65 (91.22)	1.954^{ns}	0.051
QA2	In our bank, there exists regular review on information security policy	3.58 (89.5)	3.02 (75.5)	3.44 (86.01)	5.203**	<0.001
QA3	In our bank, there exist a documented information security policy	3.67 (91.75)	3.5 (87.5)	3.63 (90.63)	0.654^{ns}	0.513
QA4	In our bank, roles and responsibilities of employees are clearly defined in information security policy	3.25 (81.25)	3.12 (78)	3.22 (80.51)	0.530^{ns}	0.596
QA5	In our bank, employees are aware of information security policies and guidelines	2.56 (64)	2.29 (57.25)	2.49 (62.35)	1.635^{ns}	0.102
QA6	In our bank, regular training programmes on information security are conducted	2.65 (66.25)	2.05 (51.25)	2.5 (62.5)	3.076**	0.002
QA7	In our bank, there exist regular risk assessment and risk management practices	3.32 (83)	3.52 (88)	3.37 (84.23)	2.077*	0.038
QA8	There exists documented recovery and business continuity plan	3.62 (90.5)	2.98 (74.5)	3.46 (86.46)	4.607**	<0.001

** significant at 0.01 level; * significant at 0.05 level; ns non-significant at 0.05 level

Mann Whitney U test was used for comparing the perception about each practice among the respondents in private sector and public sector banks. Z-value in the case of perceptions about giving high regards by top management about information security was found to be non-significant which indicates that this practice is almost same in both the banks.

Z-value corresponding to the perception on the regular review on IS policy was found to be significant at 0.01 level and the mean score was of private bank (89.5) is higher than the public bank (75.5) which shows that the private banks review their policy better than public banks. Similarly, in the case of existence of regular risk assessment and risk management practices, it was found significant at 0.05 level. But in this case, public sector banks have more value than private sector banks.

In the case of existence of documented information security policy, clearly defined roles and responsibilities of employees in IS policy and awareness of IS policies and guidelines among the employees, Z values are found to be non- significant. It shows that it is practiced almost same in both the private and public sector banks.

In the cases of conducting regular training programmes on IS and existence of documented recovery and business continuity plan, it was found highly significant. In both cases, private sector banks have higher value than public sector banks.

RESULTS AND DISCUSSION

The study was analysed by considering the following aspects:

i) Support from top management
ii) Information security policy
iii) Employees' awareness on information security policy
iv) Risk assessment and management

The study on information security management practices and the observations made from the study are greatly useful to the current banking organizations to take meaningful steps for improving the information security practices. The observations and findings are discussed below.

From the study it was observed that overall information security practices followed by the private and public sector banks are the same. While analysing the information security practices followed by the public and private sector banks in Kerala, it was observed that "top management gives high regard to information security" and "existence of documented information security policy" topped the list (Average Mean = 3.65 and 3.63 respectively).

The study also reveals that "employees' awareness of information security policy" and "conducting regular training programmes on information security" ranked the least (Average Mean = 62.5 and 62.35 respectively).

It was also noted that while comparing the private and public sector banks, in the cases of perceptions about 'giving high regards by top management on information security', 'existence of documented information security policy', 'clearly defined roles and responsibilities of employees in IS policy' and 'awareness of IS policies and guidelines among the employees', it was found that it is the same in both the banks.

While in the case of the perception on the regular review on IS policy, conducting regular training programmes on IS and existence of documented recovery and business continuity plan, private sector banks have better practices than public sector banks. On the other hand, in the case of existence of regular risk assessment and risk management practices, public sector banks have better value than private sector banks.

In general, it was observed that out of the four aspects, "employee's awareness on information security policy" has found to be of less value which indicates that banking organizations need to give more emphasis on educating about information security management and its importance to business.

SUGGESTIONS

The study was done among the public and private sector banks headquartered in Kerala, India. A structured questionnaire was used for collecting the data from the IT employees who were handling the information security management.

From the study it was observed that the information security practices followed by both the private and public sector banks are the same. The respondents agree that the top

management gives high regard to information security and information security policy. However, it is found that there exists lack of awareness on information security among the employees of both private and public sector banks and lack of training on information security from the organization side.

Hence, banking organizations must give more emphasis on educating and creating awareness on information security to the new and existing employees and should also regularly organize training programmes to the employees and evaluate on their learning on information security management.

CONCLUSION

The information security practices have been widely discussed topic in the modern banking and financial sector. The present study has been carried out to analyse the information security practices followed by the Indian banks. The study reveals that mere implementation of information security practices does not protect the system, rather banking and financial organizations should create awareness among the new and existing employees and should also provide regular training programmes on information security management practices. The study was limited to employees of IT department who were handling information security management of select banks headquartered in Kerala. Hence, future studies can be done including other employees of same banks and also in other banks across India.

REFERENCE

1. Alber, N. & Nabil, M. (2015). The impact of information security on bank's performance in Egypt. *International Journal of Economics & Finance*, 7(9), 219-225. DOI: 10.5539/ijef.v7n9p219

2. Ambhire, V.R. & Teltumde, P.S. (2011). Information security in banking and financial industry. International Journal of Computational Engineering & Management, 14, 101-105.

3. Baskerville, R., Spagnoletti, P. & Kim, J. (2014). Incident -centred information security: Managing a strategic balance between prevention and response. Information & Management, 51, 138-151. http://dx.doi.org/10.1016/j.im.2013.11.004

4. Brar, T.P.S., Sharma, D. & Khurmi, S.S. (2012). Vulnerabilities in e-banking: A study of various security aspects in e-banking. *Proceedings of 'I-Society 2012' at GKU, Talwandi Sabo Bathinda (Punjab), International Journal of Computing & Business Research*.

5. Farn, K., Lin, S. & Fung, A.R. (2004). A study on information security management system evaluation – assets, threat and vulnerability. *Computer Standards & Interfaces* 26, 501-513.

6. Gonzalez, J. & Sawicka, A. (2002). A framework for human factors in information security. WSEAS International Conference on Information Security, Rio *de Janerio, Brazil.*

7. Ma, Q., Johnston, A.C., Pearson, M. J. (2008). Information security management objectives and practices; a parsimonious framework. *Information Management & Computer Security*, 16(3), 251-270. http://dx.doi.org/10.1108/09685220810893207

8. Mbowe, J. E., Zlotnikova, I., Msanjila, S. S. & Oreku, G. S. (2014). A Conceptual Framework for Threat Assessment Based on Organization's Information Security Policy. *Journal of Information Security*, 5, 166 -177. http://dx.doi.org/10.4236/jis.2014.54016

9. Mishra, S., Dillon, G. & Richmond, F.A. (2006). Information systems security governance: a behavioural perspective. Semantic Scholar. 18-26. https://pdfs.semanticscholar.org/3f74/9f754d05d7a46a2e4f39fd019c1d00b54323.pdf?

10. Nazareth, D.L. & Choi, J. (2015). A systems dynamics model for information security management. *Information & Management*, 52, 123 -134. http://dx.doi.org/10.1016/j.im.2014.10.009.

11. Priya Elizabeth Issac and S. Venkatachalam "Human Resource Information Security Threats: The Indian Banking Context " Journal of Advanced Research in Dynamical & Control Systems, Vol. 10, 12-Special Issue, 2018. ISSN 1943-023X.

12. Salgovicova, J. & Prajova, V. (2012). Information Security Management. *Research Papers Faculty of Materials Science and Technology Slovak University of Technology* 20, 114-119.

13. Siponen, M. & Willison, R. (2009). Information security management standards: problems and solutions. *Information & Management*, 46 (5), 267-270. https://doi.org/10.1016/j.im.2008.12.007

14. Stewart, S. and Jurjens, J. Information security management and the human aspect in organizations. *Information & Computer Security* 25 (5) (2017) 494-534.

15. Wawak, S. (2010). The importance of information security management in crisis prevention in the company. *The Conference Proceedings of 6th International Symposium on Business Administration Global Economic Crisis and Changes Restructuring Business System: Strategic Perspectives for Local, National and Global Actors.* https://www.researchgate.net/publication/285158174

16. Yildirim, E. Y. (2016). The importance of risk management in information security. *Proceedings of The IIER International Conference, Rio de Janerio, Brazil, 5-8.* http://www.worldresearchlibrary.org/up_proc/pdf/543-14829057935-8.pdf