ISSN: 2321-7782 (Online)
Impact Factor: 6.047

Volume 4, Issue 9, September 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

A Critical Review on Information Security Threats Faced by Indian Banks

Nisha Ann Jacob[1]
Research Scholar, Department of Management Studies,
Karpagam University, Coimbatore, Tamil Nadu &
Assistant Professor at De Paul Institute of Science and Technology,
Angamaly, Kerala – India

Dr. George V. Antony[2]
Dean,
FISAT Business School,
Angamaly,
Kerala – India

***Abstract:** Information thefts in banks have becomes the order of the day. Viruses, worms, hackers, and employee abuse and misuse create a dramatic need for understanding and implementing quality information security. Technological advances in information security are able to contain and prevent most of the remote threats to information security. This research paper is to understand the depth of social engineering related information security threats and its business impact on the banking sector.*

***Keywords:** Banking, Information Security, Information Security Threats, Business Impact.*

I. Introduction

Banks in India made tremendous growth since the liberalization of the economy in 1990s. Banks are at the forefront in innovation and successful implementation of new technologies which include modernization of the Payment Systems, the Automated Clearing House, the Credit Reference Bureau, the Real Time Gross Settlement Scheme, Cheque Transaction System, Currency Center Project, and sharing of their Automated Teller Machine (ATM) networks.

These advances however increase the levels of vulnerabilities within the banks and increases the avenues for exploitation considering the increasing threats and effects of insider attacks. It is now imperative for the banking industry to re-imagine information security as the insider threats increase in magnitude and complexity. According to a global economic survey GECS (2011), carried out in 78 countries to provide a global picture of economic crime, revealed that cases of information security breaches are on the rise. There are more opportunities to commit fraud and more pressure to do so. Ernst and Young's Security survey crime statistics show that a total of 84,842 white-collar crime cases were reported between April and March 2009/10, in the leading banks in India marking a 56% increase from 2006. Information security breaches and fraud are increasingly proving to be lucrative opportunities as they now cost the global corporate sector an estimated $388 billion annually. While the larger portion of this cost goes towards the security infrastructures that mitigate the threats, an estimated over 30% is direct cash lost through the information breaches and fraud (Standard Digital, 2012).

Information is one of the most important business assets that add value to an organization. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or through electronic means, shown on films, or spoken in conversation. Whatever be the form of information takes, or means by which it is shared or stored, it should always be appropriately protected (ISO 17799, 2000).

The current dynamic technological advances help to increase the importance of electronic information. Banks now perform most of their day to day business activities electronically and this resulted in drastically change in the level of information security threats. Trustworthy employees who have legitimate access to the information, deliberately or accidentally affect bank's business operations. According to Research Foundation (2006), the nature of computer crime changes over the years as

© 2016, IJARCSMS All Rights Reserved

the technology changes and this has a paved way for criminal activities. Although thrill-seeking hackers are still common, the field is increasingly dominated by professionals who steal information for sale and disgruntled employees who damage systems or steal information for revenge or profit.

External threats to information security such as- physical security breaches, network hacking attempts, viruses and spyware attacks, system sabotage, among others (Schultz, 2002) received wide publicity due to their frequency, complexity and magnitude. But according to the researchers and information security experts, attacks from the inside of the organization are considered more risky and present a bigger threat because insiders have the access and therefore the power to pounce on any vulnerability (Baker et al., 2008). They include sabotage, theft and installation of malicious and unauthorized software, social engineering, and viruses. The insider information security threats which are the basis of fraud and all other nefarious activities are not new. As far back as the 1980’s, the insider threat was real and a headache for many organizations (United Press International, 1981). According to the surveys and the research reports, the current or the former employees present the greatest information security threats. Further, the frequency and number of these insider threats increase exponentially in recent years (Greitzer et al., 2008). More concerted efforts are therefore required to prevent the insider threats from growing to unmanageable proportions which could lead to widespread economic losses among others for the modern day banks.

II. Statement of the Problem

Banking analysts infer that fraud and cyber-crime are the most apprehensive issues facing banks today. In the present banking environment, the relevance of Information Security Threats is very high because today banking operations rely on technology and also offers alternate channels for providing services. The business impact of such breach incidents is very high.

Majority of the studies about banking and specifically on information security issues in the banking domain reveals that the younger generations are more receptive to the adoption of technology banking than the older generation. Therefore, a deleted study on the information security awareness of the younger generation is highly relevant while studying about the social engineering risks that the banks, their customers and employees are exposed to. Eyong (2014), in the recent study to understand the information security awareness training to the younger generation observes that the younger generation understands the need for proper awareness on information security but most of them are keen to take efforts to enrich their knowledge level on information security. Such situations not only affect the individual concerned but also affect the banking organization they interact with.

III. Review of Literature

The business environment today is undergone with tremendous transformation for the past few years. These accelerated transformations are highly visible in the financial services industry and banking in particular. With the advent of internet technologies especially after 1995 banking organisations around the world using the technological applications heavily not only in the banking operations but also in the customer service and related areas. There are many empirical research initiatives carried out on the technological adoptions in the banking sector. Some of the studies like Sathye (2003), Weng, et al. (2006), Gupta, et al. (2007), Safeena,et al. (2010), Bamoriya, et al.(2012) discuss various aspects related to the use and applications of internet enabled technological solutions in the banking organisations. While majority of the research initiatives focused on the benefits of the use of technological applications in the banking organisations, few studies also tried to examine the challenges and problems associated with the use of technology in the banking.

Further, Ashban and Burney (2001) and Bradley and Steward (2002) explained the relative adoption of tele banking and internet banking among the banking customers. However, majority of the banking organisations today, promote the use and adoption of mobile banking among their customers as it is considered to be the most cost effective mode of banking transactions. Such improved and fast adoption of internet enabled banking technologies bring many concerns to the banks as well as to the customers. These concerns include the issues related to the privacy of personal and financial information of the customers, security of the person, leakage of vital information, misuse of customer data, phishing and social engineering related information security threats.

In the modern business environment, majority of the population are actively involved in social networking sites and platforms. Such situations offer effective and fruitful environment for the criminals and people with polluted mind to use the social media in sourcing the vital information's from the banking organisations. Some of the research initiatives on information security explain the acceptance of technological adoptions by the younger generations. However, very less evidence is available about the high level of awareness of these young population on information security related threats and risks. It is also understood that the poor awareness of these user groups and their passive approach towards information security exposes them to many social engineering related issues.

Margaret and Kathrine (2012) in their research initiative on student's perception of bluetooth security reveal that majority of the younger generation fail to take adequate precautions to mitigate against threats and related vulnerabilities. The study also reveals that the awareness level on information security varies among the respondents.

Deepa et al. (2014) conducted a study about the information security issues in the Australian context and discussed that the online presence of organisations creates security related threats and also explained the importance of creating security awareness while managing the risks.

The recent research initiative and the critical analysis on information security research by Mario and Andrea (2014) reviewing over one hundred and sixty four theories and about six hundred and eighty four publications reveal that majority of the studies are subjective and argumentative category. The study also identifies the existing gaps and suggested areas for the future research. The body of knowledge on information security research shows few studies on social engineering related information security threats and risks.

Stefan et al. (2014) investigated the latest challenges in information security risk management to provide an insight about the current risk management approaches and brings out the commonalities and differences of the different approaches. The study concludes that the identified risk management approaches are not fully support mechanisms to help decision makers while deciding on risk and cost trade-off. , Petros et al. (2005) explored the sources of information systems security knowledge and the critical role of information systems security management systems in the organisations. The study points out that the successful security management of an organization strongly depends on the active involvement of the users and other stakeholders while planning, analyzing, designing and implementing the organizational information system. The research also brings out an interesting observation that most of the stakeholders fail to have adequate knowledge of information system security related aspects.

Suhazimah and Ali (2012) conducted a study on assessing information security maturity in the Malaysian context using quantitative approach. It reveals that the two variables risk management and individual perception are found to be discriminating between the enterprises that have high and low levels of information security management practices.

Majority of the studies on information security conducted in the recent times elaborately discuss the sophistication of social media and points out the fragileness of the social media in terms of cyber related attacks. Wu (2013) administered a recent survey on information security risks of mobile social media through blog mining and extensive literature search. The study categorically identifies various risks related to mobile social media and further suggests good practices that would be useful for enterprises while mitigating the information security concerns and associated risks related to social media attacks.

IV. Scope of the Study

This study focuses on exploring the approach and awareness of the bank employees towards social engineering related information security threats. The study is restricted to banks headquartered in Kerala. So the study covers only those IT employees working in State Bank of Travancore, Federal Bank, South Indian Bank, Catholic Syrian Bank and Dhanalakshmi Bank.

V. Objectives of the Study

1. To examine the information security threats in terms of technology related information security threats, human related Information Security Threats and organisational vulnerability.
2. To understand the number of occurrences of the Information Security threats and the resultant business impact on the Banks.

VI. Methodology

The feasibility and reliability data collection has high relevance and impact on the successful completion of a research initiative. Further, the area of study is also a decisive factor in finalising the sample framework. As the study focuses on social engineering related information security threats in the banking which is deemed to be highly intrusive in nature, the possibility of collecting accurate and appropriate data from the respondents seems to be challenging. The multiple discussions with the senior banking experts, information security professionals and experienced academic researchers give insights to the researcher in finalising the sampling method to be institutionalised for the study. Accordingly, the researcher finalises the sampling method based on the following assumption's and conclusions.

a) The identified sample is a member of the Indian Bankers Association,

b) The select sample is head quartered in Kerala State,

c) The identified sample has acceptable level of technology adoption, and

d) The select sample offers alternate banking channels apart from the branch banking.

Therefore, in line with the above cited assumptions, the researcher decides to include all five public and private sector bank in the sampling framework namely State Bank of Travancore, Federal Bank, South Indian Bank, Catholic Syrian Bank and Dhanalakshmi Bank.

The study employs with survey method as the research approach. The data for the study is collected through structured questionnaire from the IT employees of the responding banks. The secondary data was sourced from research journals, web sites of the banks, Reserve Bank of India published sources and other relevant sources.

VII. Results and Discussions

The study tries to categorise the information security threats into various aspects primarily to understand in terms of three broad dimensions namely,

a) Human related information security threats,

b) Technology related information security threats, and

c) Organisational vulnerability related aspects.

Among the various technology related information security threats faced by the banks, it is seen from the study that threats related to computer virus are more visible (79.2 %) among the responding banks. Further, threats due to malware and spyware also cause major concerns (74.4%) to the responding banks. However, the study shows that threat due to application / middleware vulnerability (63.2%) and poor patching of applications & OS (52.8%) also affects the responding banks.

It has to be noted that 69.6% of the respondents state that BYOD concept does not create information security threats to the responding banks. The responding banks also explain that their bank (64%) also experiences instances of attacks due to organised crimes in the digital space. Another major aspect that positively contributes to information security threats to banks is the lack of employee awareness on information security. 63.8% of the respondents vouch for the same through their response. In majority of the responding banks, it is seen that sharing of user id and password (56%) is reported to be critical information security related concerns of the responding banks.

Table 7.1 Occurrence of Technology related Information Security Threats faced by the Indian Banks

Threats	No. of occurrence			
	0	1 to 5	6 to 10	> 10
Mobile devices and BYOD	87 (69.6)	38 (30.4)	(0)	(0)
Malware & spyware	32 (25.6)	71 (56.8)	22 (17.6)	(0)
Application / middleware vulnerability	46 (36.8)	66 (52.8)	13 (10.4)	(0)
Poor patching of applications & OS	59 (47.2)	38 (30.4)	24 (19.2)	4 (3.2)
Computer virus	26 (20.8)	59 (47.2)	33 (26.4)	7 (5.6)

Values in the brackets are percentages

Source: Survey Data

The study tries to explore the organisational vulnerability related information security threats faced by the banks. It is seen that lack of adequate training and education (52.8%) is reported as the major concerns of the responding banks. Further, it is explained that the aspects like poor information security culture and inadequate management support towards information security is also contributing to information security threats in the responding banks. When explores about the level of severity of occurrence of information security threats, it is seen from the study that the severity observes to be moderate (16%) or low (84%) and is observed to be within the acceptable tolerance limit.

Table 7.2 Occurrence of Organisational Vulnerability related Information Security Threats faced by the Indian Banks

Threats	No. of occurrence			
	0	1 to 5	6 to 10	> 10
Lack of adequate training and education	59 (47.2)	56 (44.8)	10 (8)	(0)
Poor information security culture within the bank	74 (59.2)	44 (35.2)	7 (5.6)	(0)
Inadequate management support	87 (69.6)	38 (30.4)	(0)	(0)

Values in the brackets are percentages

Source: Survey Data

It is also seen from the study that 55.2% of the banks state that they face information security threats due to the irresponsible behaviour and approach of the employees towards their information security responsibility. Even though banks face some amount of security related threats due to the behaviour of disgruntled employees (37.6%) and internal data leakage (31.2%), threats from the information security breaches from the outsourced partners (26.4%) is reported negligible.

Table 7. 3 Occurrence of Human related Information Security Threats faced by the Indian Banks

Threats	No. of occurrence			
	0	1 to 5	6 to 10	> 10
Organized crime in digital domain	45 (36)	61 (48.8)	19 (15.2)	(0)
Disgruntled employees	78 (62.4)	41 (32.8)	6 (4.8)	(0)
Data leakage (internal)	86 (68.8)	34 (27.2)	5 (4)	(0)
Outsourced partner breaches	92 (73.6)	33 (26.4)	(0)	(0)
Lack of Information Security awareness of employees	46 (36.8)	46 (36.8)	27 (21.6)	6 (4.8)
Irresponsible employee behaviour towards information security responsibility	56 (44.8)	38 (30.4)	26 (20.8)	5 (4)
Social engineering threats	54 (43.2)	60 (48)	11 (8.8)	(0)
Purposeful negligence of employees towards information security	40 (32)	59 (47.2)	23 (18.4)	3 (2.4)
Sharing of user id and password	55 (44)	28 (22.4)	31 (24.8)	11 (8.8)

Values in the brackets are percentages

Source: Survey Data

While analysing the business impact (BI) of the technology related information security threats, it is seen that BI is high in case of threats like mobile devices and BYOD and computer virus. However, the occurrences of threats related to malware & spyware, application/ middleware vulnerability and poor patching of applications & OS also cause threats with high business impacts.

While looking at the business impact from the human related information security threats if it is seen that threats arising from aspects like sharing of password and user id, lack of employee awareness on information security and irresponsible behaviour of the employees towards their information security responsibilities have greater business impact among other human related aspects. Organised crime in the digital cyber space is also a great concern to the banking organisations in terms of business impact.

It is seen from the study that business impact due to the poor information security culture creates more business impact than other organisational vulnerability related information security threats. It is learned from the study that about 14.4% cases of high business impact, another 18.4% cases of medium business impact and about 67.2% cases of low business impact from the various information security incidents reported by the responding banks.

Further, looking at the overall information security breach incidents namely human, technology related and organisational vulnerability related ones, it is seen that the aspects like inadequate management support, lack of adequate training and education, sharing of user id and password, irresponsible behaviour of employees towards their information security responsibility, lack of awareness on information security and use of mobile devices and BYOD are the concerns of the responding banks.

VIII. Conclusion

Among the human, technology and organisational related information security threats faced by the responding banks, it is seen that human related threats pose more security issues when comparing to other types of threats. Therefore, there is an urgent need for employee orientation and reorientation to address this critical issue. Banks have to understand this issue with atmost importance and implement effective training and education programmes on information security. A provision to evaluate the information security related knowledge of the employees has high relevance in minimising the occurrence of such incidents and its business impact.

References

1. Al Ashban, A. A. & Burney, M. A. 2001. Customer adoption of tele-banking technology :the case of Saudi Arabia. International Journal of Bank Marketing. Vol. 19 (5), pp. 191-200.
2.] Bradley, L. & Steward, K. 2002. A Delphi study of the drivers and inhibitors of Internetbanking. International Journal of Bank Marketing. Vol. 20 (6), pp. 250-260
3. Margaret Tan, Kathrine Sagala Aguilar, (2012) "An investigation of students' perception of Bluetooth security", Information Management & Computer Security, Vol. 20 Issue: 5, pp.364 - 381
4. Deepa Mani , Kim-Kwang Raymond Choo , Sameera Mubarak , (2014) "Information security in the South Australian real estate industry: A study of 40 real estate organisations", Information Management & Computer Security, Vol. 22 Issue: 1, pp.24 - 41
5. Mario Silic, Andrea Back , (2014) "Information security: Critical review and future directions for research", Information Management & Computer Security, Vol. 22 Issue: 3, pp.279 – 308
6. Stefan Fenz, Johannes Heurix, Thomas Neubauer, Fabian Pechstein, (2014) "Current challenges in information security risk management", Information Management & Computer Security, Vol. 22 Issue: 5, pp.410 - 430
7. Petros Belsis, Spyros Kokolakis, EvangelosKiountouzis, (2005) "Information systems security from a knowledge management perspective", Information Management & Computer Security, Vol. 13 Issue: 3, pp.189 - 202
8. Suhazimah Dzazali, Ali Hussein Zolait, (2012) "Assessment of information security maturity: An exploration study of Malaysian public service organizations", Journal of Systems and Information Technology, Vol. 14 Issue: 1, pp.23 – 57