Employee Awareness on Social Engineering Information Security Threats: The Indian Banking Context

Nisha Ann Jacob¹, Dr. George V. Antony²

¹Research Scholar, Department of Management Studies, Karpagam University, Coimbatore, Tamil Nadu and Assistant Professor at De Paul Institute of Science and Technology, Angamaly, Kerala, INDIA
²Dean, FISAT Business School, Angamaly Kerala, INDIA

ABSTRACT
The management of Information assets is one of the prime concerns of modern day banks. Awareness about the risks helps to develop healthy practices that restrict information security issues in the banks. This study is an attempt to understand the awareness and approach of the bank employees about information security threats and risks.

Keywords--- Information Security Threats, Social Engineering Threats, Awareness on Security Threats

I. INTRODUCTION
The adoption of internet enabled technologies in banking brings newer security threats to the banks as well as to the customers. The management of information assets becomes one of the prime concerns of modern day banking enterprises. The concept of social engineering is engaged as an effective tool by the criminals for sourcing the personal and financial information of the banking customers. Even though there are many studies available in the literature at the international scenario on information security, very few research initiatives are carried out in the Indian context especially in the banking sector. Most of the studies report in the literature are generally generic in nature. George (2010) carried out a specific study on information security policy management in the Indian banking sector. It reveals that majority of the information security threats faced by a bank are internal in nature and human initiated one. Irrespective type of risks and threats they face, such incidents create uncertain environments and unhappy situations. Earlier studies on information security conducted across the world by many researchers observed that better awareness about the risks and information security positively contribute to healthy practices that restrict information security incidents in organisations. It has high relevance in the financial services industry especially in the banking sector.

II. STATEMENT OF THE PROBLEM
In the present banking environment, the relevance of Social Engineering 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 are very high. Prior studies arrived at a conclusion that proper awareness of bank executives regarding the social engineering information security threats and their business impact would help to reduce the number of their occurrence and also its business impact.

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 Sathyne (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 focus 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.

Iwan (2013) carried out a study on raising risk and security related awareness against social engineering using the theory of planned behavior. Aspects like perceived behavioral control, attitude and social norms were identified as the major variables in the study. The rapid adoption of the internet technologies and related applications in business bring multidimensional information security threats. The familiarity and usage pattern of the social media and platforms of the individuals also increase the security risks related to social engineering.

The social engineers always attach the weakest link in the chain. The prior research initiatives carried out by the earlier researchers opine that, the social engineers establish relationship with the individuals disgusting their identity and steel vital information for doing fraudulent transactions. It is observed that the social engineers also attack employees of the organizations by manipulating their identity and cause damages to the organization and society. Richard et al. (2012) extended the study on social engineering with an objective to raise awareness of social engineering and reducing the social engineering incidents. The study reveals that most of the organizations recognize the importance of exercising internal controls and concludes that these organisations fail to appropriately understand the dangers associated with these social engineering attacks. Mannmohan et al. (2014) conducted a study on the issues of information security in the Indian context using Delphi method and suggested a framework for managing information security that further provide managerial insights in handling information security related issues.

Tamura et al. (2009) investigated the susceptibility of the employees towards social engineering in corporate enterprises and concluded that most of the responding employees lack at the basic level of security awareness. The study emphasizes the need for raising the information security awareness. Efthymia et al. (2014) researched on the association of awareness of human factor and information security considering five human factors and nine information security related attacks. The study brings out meaningful outcome by discussing the critical importance of awareness about information security. Euripidis and Diomidis (2001) examined the information systems security in the Greek public sector enterprises and explained the importance of proper training and the relative importance of the human resources in the enterprise in achieving high levels of information systems security.

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 bank 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 understand the awareness and approach of the bank employees about social engineering information security threats and risks.
2. To develop insights on employees’ approach towards social engineering information security threats by analysing various demographic factors.

VI. METHODOLOGY

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

Assessment of the awareness of the employee and impact of the threats on business of the bank is done by computing the total scores for each. For this, a score is given to each statement in the awareness as 0, 1, 2, 3 and 4.
respectively to the response strongly disagree, disagree, no opinion, agree, strongly agree and for each statement related to impact as 0, 1 and 2 respectively to the response Low, Average and High. The total scores are converted to percentage scores by dividing the total score by maximum expected score and multiplying by 100. Then the expected range of the percentage score is 0 to 100. This expected range is divided into three equal classes in such way that the respondents having scores in between 0 to 33.3, those having scores in between 33.3 to 66.7 and the respondents having response greater than or equal to 66.7. The assessment of severity of concurrence of overall information security threats is also done in the same way.

VII. RESULTS AND DISCUSSIONS

The study shows that there existing marginal difference in the awareness level of social engineering related information security threats between the public and private sector banks. The result shows that the employees of the public sector banks have higher level of awareness than the private sector banks which is very marginal in nature. An effort is made to analyse the awareness level of the respondents based on their professional experience. It is seen that exists significant difference in the awareness among the employees having different experience levels. The study shows that those who with 11-15 years of experience having significantly higher awareness on social engineering related information security threats when comparing to all other groups. But, it is also observed that employees belong to more than 15 years of experience have the lowest level of awareness while comparing to employees having 5 to 15 years of experience. It is also seen that employees with post-graduation exhibit the better level of awareness than the graduates and others.

Table 7.1 Comparison of Level of Awareness among the respondents having different experience

<table>
<thead>
<tr>
<th>Experience</th>
<th>N</th>
<th>Mean</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 5 years</td>
<td>61</td>
<td>59.819</td>
<td>6.4954</td>
</tr>
<tr>
<td>5-10 years</td>
<td>75</td>
<td>60.306</td>
<td>6.4294</td>
</tr>
<tr>
<td>11-15 years</td>
<td>53</td>
<td>65.664</td>
<td>5.5833</td>
</tr>
<tr>
<td>&gt;15 years</td>
<td>141</td>
<td>57.979</td>
<td>5.3302</td>
</tr>
</tbody>
</table>

F-value = 22.176; P-value < 0.001

Source: Survey Data

** Significant at 0.05 level

Means having same letter as superscript are homogeneous

The study shows that almost all respondents states the information assets of the bank has to be protected, while only 71.5 percentage of the employees opines that the information assets are vulnerable. It is observed that 82.1 percentage of the respondents feel that adequate protection of the information infrastructure restrict any unauthorized access to bank’s information assets. However the study shows a different picture regarding the bank employee’s opinion on the efforts of their bank in protecting the information assets and guarding against the social engineering security threats. Almost 95.5 percent of the employees feel that their bank take appropriate measured on protecting the information assets. But, only 85.4 percentage is confident that their bank take adequate protection against social engineering related information security threats.

The success of information security governance initiatives depends on various related aspects including the employee approach towards information security, their awareness about compliance, organisational policies on non-compliance, the efforts taken by the management towards information security etc. It is seen that 91.2 percentage of the employees feel that they need to comply with the information security requirements of the organisations. However, it is revealed that only 59.4 of the respondent’s bankers are aware about the penalties applicable to non-compliance to information security responsibilities. Even though 99.1 percentage of the bank employees feel the need for training on information security related aspects, it is revealed that 75.2 percentage of them have an opinion that they should attend all the training programmes.

Finally, for assessing level of awareness first worked out a total score by adding the scores of each statements. Scores are given to each statement as 0, 1, 2, 3 and 4 respectively to the response strongly disagree, disagree, no opinion, agree, strongly agree. Then the total score is first convert to percentage score. Expected range of the percentage score is 0 to 100. This expected range is divided into three equal classes in such way that the respondents having scores in between 0 to 33.3 belongs to low aware group those having scores in between 33.3 to 66.7 belongs to average aware group and the respondents having response greater than or equal to 66.7 belongs to high aware group. Classification according to that is given in table 7.2
Table 7.2 Perception about Level of Awareness

<table>
<thead>
<tr>
<th>Level</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Average</td>
<td>282</td>
<td>85.5</td>
</tr>
<tr>
<td>High</td>
<td>48</td>
<td>14.5</td>
</tr>
<tr>
<td>Total</td>
<td>330</td>
<td>100</td>
</tr>
</tbody>
</table>

Source: Survey Data

Hence, it is seen that 85.5% of the responding bank employees have average level of awareness on information security and related information security threats where the remaining 14.5% percentage of them show high level of information security awareness.

VIII. CONCLUSION

The study shows that the employees of the banks show the positive approach towards information security especially related to social engineering. However, evidences show that their practices are not in line with their attitude and approach towards information security. The need of quality training programmes on these critical aspects is highly emphasised as lack of adequate information on these aspects may cause severe breach incidents that may cause severe business impact to the banks. Therefore, there is a huge responsibility for the banks while designing the training programmes. The banks shall take efforts to see that they include contents on social engineering related information in the instructional design for the employees so that the employees have good knowledge on these latest developments in which such a situation mandates redesign the training and education programme on information security so that effective methodologies and systems can be designed to bring out better results in terms of employee acceptance and practices.

Since the concept of social engineering related information security threats has growing importance it will be appropriate if Reserve Bank of India initiate a project to create awareness on information security, especially about social engineering related information security issues among the banking employees and customers as it is primarily a social concern. Such a platform shall raise the knowledge level of the banking stakeholders on social engineering related information security threats and related issues.

REFERENCES