Information Security Awareness: Case Study In Stock-Broking Company

Faizatul Akma Mohd Adnan, Rasimah Che Mohd Yusoff, Nurazean Maarop, Norziha Megat Zainuddin, Roslina Ibrahim

Advanced Informatics School, Universiti Teknologi Malaysia, Kuala Lumpur

mfaizatulakma@yahoo.com

Abstract. Stock-broking company handled sensitive data or information of client’s financial instruments. However, lack of security awareness among staff who handle the client’s data has the potential to cause data breach or information violation. The study was conducted to determine the information security awareness among staff at a universal stock-broking company in Kuala Lumpur. The model of information security awareness was developed using the constructs confidentiality, integrity, availability and knowledge. The quantitative method using a set of questionnaire was performed. Eighty four respondents participated in this study. The results revealed that confidentiality, integrity and knowledge significantly related with information security awareness while availability not significantly related.

Keywords: information security awareness, confidentiality, integrity, availability, knowledge and stock-broking.

INTRODUCTION

A stock-broking company conducts trading of client’s financial instruments such as shares, warrants, and options, besides investment advisory services, nominee services and institutional share dealings. In Malaysia, a universal stock-broking company is formed by a merger with or acquisition of at least three other stock-broking companies and it has fulfilled the qualifying criteria set out by the Securities Commission of Malaysia. Being one of the capital market participants the business nature of a universal stock-broking company centers on monies and financial instruments (PM Securities, 2013). Therefore information security is important to safeguard the confidentiality of clients. Previous research works show that insurance companies and stock-broking firms are at the top the percentage in data breaches (Gatzlaff & McCullough 2010, Turban et al. 2005). Many organizations or companies are unable to protect the security of information because their staffs are not aware of their responsibilities and roles in relation to the organization mission (NISTP SP 800-50, 2003). Besides that, the staff also are unable to understand or not being aware of the organization’s or company’s IT security practices and procedures. This paper will reveal the information security awareness among staff at a universal stock-broking company in Kuala Lumpur.
RELATED WORKS

Information Security Awareness

Information security awareness can be defined as the knowledge and attitude members of an organization possess regarding the protection of the physical and especially, information assets of that organization (Heru and Mohammad, 2012). The goal of information security is to ensure business continuity and to minimize business damage by preventing and minimizing the impact of security incident (Posthumus and Solms, 2004). Information security awareness is the common issue in any information system (IS) security management. Organization must be made to realize the importance of building up information security awareness, in order to ensure that information security accidents can be avoided. Any effort that is related to information security awareness usually involves the change of behavior of the end-users or the reinforcement of good security practices amongst the users.

Factors Influence Information Security Awareness

The rapid yearly growth of information makes awareness on the information security becoming more important as each year passes by. Many influencing factors have been identified in information security awareness such as confidentiality, integrity and availability (Tvrdikova, 2008). Based on Ping (2010), the behavior of end-users and their knowledge are also the factors that influence the information security awareness. The confidentiality in information assurance can be considered as the computer related assets which are accessible by authorized parties only (Pfleeger and Pfleeger, 2007). In stock-broking, there are many documents that are considered as secret and confidential, such as personal information, bank account statements, trade secrets, investment-information and others (Chia, 2012).

Integrity in information security can be defined as the correctness of the computer assets, such as the data that are used by authorized user, and in addition to that, the data cannot be in any way modified by the unauthorized parties (Pfleeger and Pfleeger, 2007). The integrity of information is very important, in order to clarify the degree of correctness of the information. Any incorrectness in term of information value can give huge negative impact to both the client and the organization such as the loss of customers’ confidence in the services offered and loss of business partners (Chia 2012; Carlson 2001). The availability in information assurance can be defined as the computer related assets that are accessible to authorized parties at appropriate times (Pfleeger and Pfleeger, 2007). The data or information must be made available when authorized users request for access without any delay, because the data or information becomes only valuable when the authorized user gets it at the right time (Naboulsi et al., 2003). Knowledge can be defined as end-user understanding of the information security which is crucial in the protection of the information since decision and action can be implemented based on the knowledge (Ping 2010; Peng and Xiong 2006; Davenport and Prusak. 1998).
PROPOSED MODEL FOR INFORMATION SECURITY AWARENESS

The proposed model for the information security awareness in stock-brokering company consist of the following constructs: confidentiality, integrity, data availability and knowledge. The hypotheses are:

H_A1: There is significant relationship between confidentiality and information security awareness
H_A2: There is significant relationship between integrity and information security awareness
H_A3: There is significant relationship between availability and information security awareness
H_A4: There is significant relationship between knowledge and information security awareness

Figure 1 shows the proposed research model.

RESEARCH METHODOLOGY

The quantitative method using a survey questionnaire was performed for this study.

Research Design

The research was conducted with employees at a universal stock broking company in Kuala Lumpur, Malaysia. A survey questionnaire was used as the instrument.

Population and Sampling

The estimated population for this study is 120. All the employees are selected based on their involvement with clients’ data in their daily routine. Due to the small number in population size, the survey questionnaire was distributed to all respondents in the population.

Measures

The survey questionnaire instrument consists of part A and B. Part A is mainly on the demographic questions about the respondent’s gender, age, education background, working position, working experience and information security awareness training attended. Part B consist of 30 questions on information security awareness, which has been adapted to suit the needs for a universal stock-brokering company. The questionnaire...
is using the 5-point Likert scale with the following responses: Strongly disagree = 1, disagree = 2, not sure = 3, agree = 4, strongly agree = 5.

Data Analysis

Descriptive analysis, reliability analysis and correlation coefficient analysis were done using SPSS version 16 for Windows.

RESULTS AND FINDINGS

Descriptive analysis has been chosen to analyze demographic profile respondents and Pearson’s correlation have been used to examine the relationship between constructs.

Descriptive Profile of Respondents

The questionnaire was distributed by hand to 120 respondents from different positions such as senior manager, executive and non-executive in a universal stock broking company. All of them have their own workstations. 84 respondents participated in this survey (70% respond rate). Table 1 shows the descriptive profile of respondents.

<table>
<thead>
<tr>
<th>Table (1): Descriptive profile of respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile of Respondents</td>
</tr>
<tr>
<td>Gender</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Age</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Working Experience</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Attended Information Security Training</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

The table showed that majority of respondents were male (62%). The age distribution of respondents showed that majority of respondents belongs into the age group of 26 to 40 years old (48%). Majority of the respondents (36%) have less than 5 years of working experience in this stock broking company. Majority of the respondents (60%) have never attended any information security training.
Reliability Statistics

The Cronbach Alpha is being used to determine the internal consistency of the questionnaire. The value was 0.773 where the reliability of the questionnaire can be considered as acceptable (George & Mallory 2009).

Correlation Coefficient and Hypotheses Testing

Table 2 shows that the summary of the hypothesis testing. The results indicated that the hypotheses $H_A1$, $H_A2$ and $H_A4$ are supported, while hypothesis $H_A3$ is not supported.

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>Results</th>
<th>Correlations</th>
</tr>
</thead>
<tbody>
<tr>
<td>$H_A1$</td>
<td>$r = 0.443$</td>
<td>Significant strong positive relationship between confidentiality and information security awareness</td>
</tr>
<tr>
<td></td>
<td>$p = 0.000$</td>
<td></td>
</tr>
<tr>
<td>$H_A2$</td>
<td>$r = 0.650$</td>
<td>Significant strong positive relationship between integrity and information security awareness</td>
</tr>
<tr>
<td></td>
<td>$p = 0.000$</td>
<td></td>
</tr>
<tr>
<td>$H_A3$</td>
<td>$r = 0.155$</td>
<td>No significant relationship between availability and information security awareness</td>
</tr>
<tr>
<td></td>
<td>$p = 0.159$</td>
<td></td>
</tr>
<tr>
<td>$H_A4$</td>
<td>$r = 0.364$</td>
<td>Significant strong positive relationship between knowledge and information security awareness</td>
</tr>
<tr>
<td></td>
<td>$p = 0.001$</td>
<td></td>
</tr>
</tbody>
</table>

CONCLUSION

The aim of this study was to evaluate the information security awareness among staff at a universal stock-broking company. The findings revealed that confidentiality, integrity and knowledge of the staffs in the universal stock-broking company significantly related with the information security awareness. This results suggesting that employees are aware of their responsibilities in maintaining confidentiality and integrity of the business information and resources. Feedbacks from users indicate that they have necessary knowledge in handling information security issues, such as phishing email. Availability showed no significant relationship with information security awareness. The stock-broking company should play a role in educating and improving employees’ understanding on the important of data availability where valuable data must be made available when needed.

REFERENCES


8. NIST SP 800-50 (2003), National Institute of Standards and Technology (NIST), Building an Information Technology Security Awareness and Training Program (NIST SP 800-50), US Department of Commerce, Washington, DC.


