Paper ID 227

Evaluating the Information Security Awareness (ISA) of Employees in the Banking Sector: A Case Study

Asanka D Dharmawansa[1#] and RAM Madhuwanthi[2]

[1]*Department of Industrial Management, Wayamba University of Sri Lanka*
[2]*Esoft Metro Campus, Kurunegala*

[#] asankad@wyb.ac.lk

Abstract: Information has become a vital and valuable asset to an organization. In the banking sector, employees should have a better knowledge about the security of the information system since they are always exposed to very confidential and sensitive information. Thus, the awareness on information security has become a major area that should be focused on by the employees as well as the management of the banking industry. The objective of this research is to evaluate the awareness of the employees on information security in the banking sector in Sri Lanka. This study is based on Human Aspects of Information Security Questionnaire (HAIS-Q). A questionnaire was developed based on relevant literature for collecting data in the study. Regression analysis was carried out using SPSS to analyze the collected data. It was concluded that all the factors in HAIS-Q are predictors of employee information security awareness (R^2= 0.984). Although all the variables have affected positively on the awareness on information security in the banking sector, the variables of Password Management, Email Use, Internet Use and Incident Reporting have a positive and significant impact on the awareness of employees on Information Security. Especially the Password Management significantly impacted on the awareness of information security. The employers should identify the importance of password management, Email Use, Internet Use and Incident Reporting when they structure training activities for employees in the banking industry.

Keywords: Information Security, Awareness, Banking Sector

Introduction

With the globalization, Information Security Awareness (ISA) has become a key concept in information security. Contrary, attackers also concern more about enhancing their capabilities by developing various novel attack methods. When they got a chance, they targeted to intend information system and effectively exploit corporate network and infrastructure through individual human behaviour. Therefore, cybersecurity has become a business problem that should concern by Chief Information system officers in every organization. The objective of ISA is to allow every employee to inform that they are vulnerable in providing opportunities for attackers to threaten the organization's corporate system and infrastructure and when they have an idea about this issue. Employees can change their behaviours to mitigate those risks and threats.

The ISA is typically focused on two aspects; understanding and compliance. According to the Kruger & Kearney, (2006) understanding means how far employees in the organization recognize the value and vitality of information security, the levels are information security appropriate to the company and what extent they have known the individual security responsibility. The other aspect; compliance is a level of commitment that concerned with information security plans, directions and strategies as per demonstrated by the

agreement (Siponen, 2001). Accordingly, ISA can be explained as employee's understanding of the companies Information Security strategies and measures and their perspective towards having to adherence to them.

Not only technological reasons but also the behaviour of computer users impact on issues of Information security (Furnell, et al., 2006, Herath & Rao, 2009, Vroom & Von Solms, 2004). Human Aspects of Information Security Questionnaire (HAIS-Q) is a well-known instrument which was developed to assess the employee's information security awareness.

In the banking sector, employees should have more knowledge about the information system security since they always exposed to very confidential and sensitive information. Therefore, awareness of the information systems in an organization and its security has become a major area that should be focused by employees as well as management of the organization. The study will use the Human Aspects of Information Security Questionnaire (HAIS-Q) as a model to evaluate the information security awareness of employees who are working in the banking sector in Sri Lanka.

The primary objective of this research is to evaluate the information security awareness of employees in the banking sector in Sri Lanka.

Literature Review

Information security is identified as the protection of the confidentiality, integrity, and availability of the data that is stored in a computerized environment (Kruger, 2006). Along with the other business assets information requires protection to make sure that the information is available in a confidential situation along with its integrity is preserved where it is necessary (Microsoft, 1999). There are various types of threats that can happen in information security. They are such as fraud, drafts, viruses, social engineering risks on protecting information etc; (Microsoft, 1999). These threats along with the careless human errors that can happen in the security controls may lead to major financial and reputational damages to the organization which can impact in the long-run. The controls need to be done along with the organizational security goals and objectives to minimize the risk that can happen.

Information security is identified as a critical and complex task and it is not just using user names and passwords as a measure of security. For many years, information security programs are more focused towards technical solutions such as firewalls, anti-virus programs, access controls etc. than in human element. Information security mainly focuses in maintain confidentiality, integrity and availability of information for the organization to perform its business operations smoothly without interruption (Kruger & Kearney, 2006). Confidentiality is defined as the protection of data and information without exposure to unauthorized parties (Mcleod & Schell, 2008). Integrity is the accurate representation of data information between the parties that disclosed them while the availability of information means provide authorized people to access relevant data as they want and when they want. Human behaviour is very important when considering the information security awareness that the employee obtains and it is not entirely depending on technical solutions (Cox, et al., 2001). In 2018, Kruger and Kearney developed a model based on social psychology field for determining information security awareness through different factors; knowledge, attitude and behaviour (KAB) and the refined version of KAB model is HAIS-Q employee

information security awareness component.

Knowledge: Knowledge can be defined as all information that an individual owns about a specific field Through the empirical review of literature that was performed the researcher has identified models, instrument and then variables for the study to accomplish the research objective.of study (Alexander & Jetton, 2000). Knowledge compromise three forms; declarative, or knowing what, procedural, or knowing how, and conditional, or knowing when and why.

Attitude: Attitude can be defined as mental and neural readiness which direct individual's all activities (Allport, 1967).

Behaviour: According to most psychologists, Behaviour is an observable action. The fundamental definition of behaviour is how people or group of people responds to a certain set of conditions.

The information security awareness is measured through HAIS-Q model which consists 63 items that are categorized into 7 types; Password management, Email use, Internet use, Social media use, Mobile devices, Information handling and Incident reporting.

The original development of HAIS-Q model was inspired to gain the understanding of employee information security awareness who are working in the government sector, Australia (Parsons, et al., 2014). The main conclusion that derived through the discussions held with senior managers of the Australian government is that the security breaches commonly happened due to the human errors along with their ignorance. This finding was the basic question that motivated for the development of HAIS-Q (Parsons, et al., 2014). Many researchers have used this model as the conceptual framework in their studies and many have tested the validity and reliability of the model (Straub, et al., 2004). HAIS-Q model can be used as a reliable measure of information security awareness (Mccormac, et al., 2016).

Information is identified as the newest currency in the current business and corporate world where the value of the business rise and falls depending on how, when, where and by whom it is been used and type of medium that is been used. Depending on the way it is used there is a risk and an opportunity in using information security. In simple terms, a user is a person who is dealing initially with the information that is related to the organization. The information security management of the organization is based on the human factor and also on the processes that are related to the organization.

Importance in creating a security culture within the organization setting arise when the human dimension of the information security is considered to be one of the weakest points. Therefore, the creation of information security culture in the organization is important in effective security management.

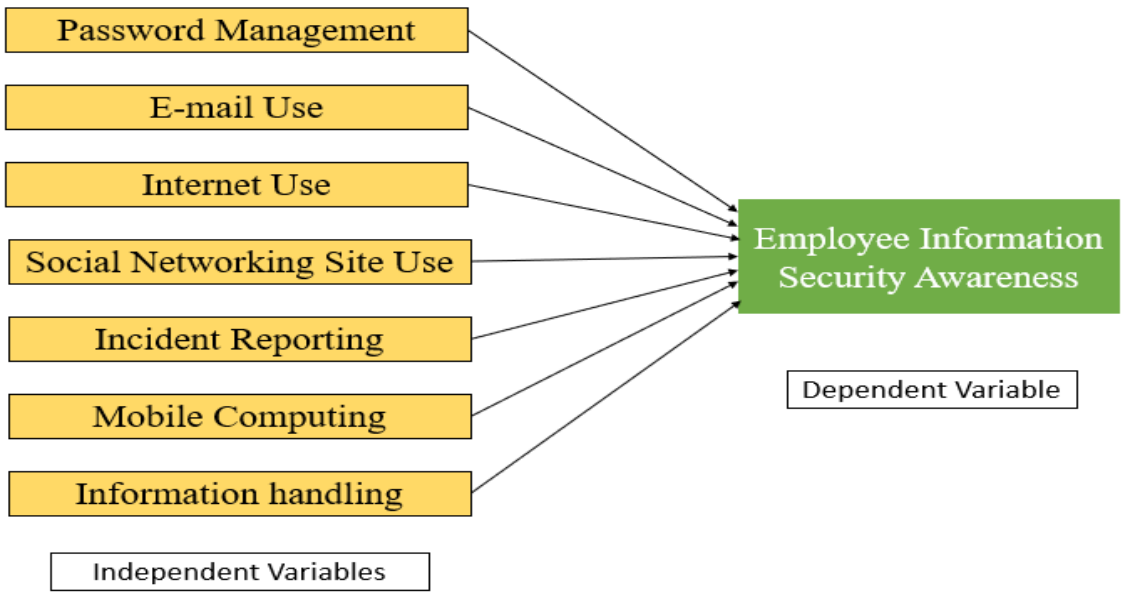

Figure 01. A Conceptual Framework

Methodology

The developed conceptual framework is illustrated in Figure 01. Seven independent variables were derived from the Human Aspects of Information Security Questionnaire (HAIS-Q), which are password management, e-mail use, internet use, social networking site use, incident reporting, mobile computing and information handling. The dependent variable of the study is employee information security awareness. Table 01 depicts the sub-areas of the selected focus areas. The Likert scale questionnaire was developed by covering all the variables of the study.

The target population of the study is all employees who work at a private bank in Sri Lanka. The sample from the above population was selected through random sampling technique. The sample size for the study is determined through the table developed by Krejcie and Morgan to fulfil the existing gap of not having a proper representative statistical sample table. Therefore, 357 employees were selected as the sample for the study.

Table 01. Sub-areas of the Focus areas

Focus area	Sub-areas
Password management	Locking workstations Password sharing Choosing a good password
Email use	Forwarding emails Opening attachments IT department level of responsibility
Internet use	Installing unauthorized software Accessing dubious websites Inappropriate use of internet
Social networking site (SNS) use	Amount of work time spent on SNS Consequences of SNS Posting about work on SNS
Incident reporting	Reporting suspicious individuals Reporting bad behaviour by colleagues Reporting all security incidents
Mobile computing	Physically securing personal electronic devices Sending sensitive information via mobile networks Checking work email via free network

Information handling	Disposing of sensitive documents Inserting DVDs/USB devices Leaving sensitive material unsecured

Result and Analysis

The descriptive analysis was illustrated as shown in Table 02. The mean value of all the variables is greater than the average and it indicates that all the factors can be affected by information security awareness.

Table 02. Descriptive Analysis

Variable	Mean	Median	Standard Deviation
Password Management	3.85	3.89	0.497
Email Use	3.99	4.00	0.511
Internet Use	3.87	3.89	0.367
Social Media Use	3.87	3.89	0.305
Mobile Devices	3.92	4.00	0.290
Information Handling	3.91	3.89	0.300
Incident Reporting	3.92	3.89	0.311
Information Security Awareness	3.69	3.90	0.584

The skewness and kurtosis values for all seven independent and dependent variables are in between -1.96 and +1.96 as shown in Table 03. It can be argued that data for both two variables are normally distributed.

Table 03. The measure of Divergence from Normality

Descriptive Statistics					
	N	Skewness		Kurtosis	
	Statistic	Statistic	Std. Error	Statistic	Std. Error
Password Management	100	-.438	.241	.366	.478
Email Use	100	-.662	.241	.122	.478
Internet Use	100	-.425	.241	-.443	.478
Social Media Use	100	-.511	.241	.032	.478
MobileDevices Use	100	-.405	.241	-.066	.478
information Handling	100	-.465	.241	-.263	.478
Incident Reporting	100	-.524	.241	-.423	.478
Information Security Awarene.	100	-.082	.241	.839	.478

Table 04. Model Summary for the predictors of information security awareness

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.992a	.984	.983	.07939
a. Predictors: (Constant)				

Table 05. Coefficients for predictors of information security awareness

Coefficients					
Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std Error	Beta		
(Constant)	-.137	.06		-	.025
Password	.548	.06	.530	8.7	.000
Email Use	.207	.05	.210	3.5	.001
Internet Use	.173	.04	.165	3.6	.000
Social Media	.018	.01	.028	1.6	.027

Mobile	.084	.06	.079	1.3	.027
information	.043	.04	.042	.93	.012
Incident	.034	.05	-.029	-	.000
a. Dependent Variable: ISA					

Table 04, illustrates the R^2 of the variable which means that 98.4% of the variance in information security awareness can be predicted from independent variables that are derived from Human Aspects of Information Security Questionnaire which are password management, e-mail use, internet use, social networking site use, incident reporting, mobile computing and information handling.

The Coefficient table (Table 05) for factors of Human Aspects of Information Security Questionnaire and Information Security Awareness provides p values of all seven independent variables. Since all values are less than 0.05 it can be concluded than all seven variables are predictors of Information Security Awareness of the employees in the private bank in Sri Lanka. Out of all seven sub-variables of Human Aspects of Information Security Questionnaire, password management is the most influential factor when predicting the information security awareness of the employees in the banking sector.

The linear model for the multiple regression equals to,

$$Y=0.548X_1 + 0.207X_2 + 0.173X_3 + 0.018X_4 + 0.084X_5 + 0.043X_6 + 0.034X_7 - 0.137$$

Where,

Y- Information Security Awareness
X_1- Password Management
X_2- Email Use
X_3-Internet Use
X_4- Social Media Use
X_5- Mobile Devices Use
X_6- Information Handling
X_7- Incident Reporting

Conclusion

The study was conducted to examine the association between seven independent variables that were derived from the Human Aspects of Information Security Questionnaire (HAIS-Q)and information security awareness of employees who are working in the banks in Sri Lanka. Through the descriptive analysis, the researcher was able to find out email use strategies used by the employees in the banks are the most commonly used aspect by them out of seven factors related with Human Aspects of Information Security Questionnaire (HAIS-Q) while other six studied factors play an equal amount of involvement is information security awareness.

Three types of independent variables; Social Media Use, Mobile Devices Use and Information Handling had a positive but moderate impact on the Information Security Awareness of employees in the banks.

Other four independent variables; Password Management, Email Use, Internet Use and Incident Reporting had a positive and strong impact on the Information Security Awareness of employees.

Password Management is the most influenced independent variable derived from the Human Aspects of Information Security Questionnaire (HAIS-Q) towards the dependent variable of employee information security awareness in the selected organization.

All factors derived from Human Aspects of Information Security Questionnaire (HAIS-Q) are better predictors of employee information security awareness in the private bank in Sri Lanka.

A. Recommendations

The number of researchers has been carried out to prove the validity and reliability of the Human Aspects of Information Security Questionnaire (HAIS-

Q) (Straub, et al., 2004 & Mccormac, et al., 2016). Hence, employee awareness on information security has become a major strength for all types of organization, findings of the study have more practical consequences. Since employees in the banking industry are working with very confidential information related to customers and the bank itself, they should follow a proper strategy with the security of information which they possess.

By administrating the HAIS questionnaire, an organization can determine the level of the awareness that employees have toward each factor such as password management, e-mail use, internet use, social networking site use, incident reporting, mobile computing and information handling. When a bank needs to perform training for employees on information security awareness, they can use this questionnaire before the study to identify the baseline of employee information security awareness and then after conducting the training they can measure the success of the training program through providing this questionnaire for employees and on the other hand, management can identify the areas that need to improve.

References

Alexander , P. A. & Jetton, T. L., 2000. Learning from text: A multidimensional and developmental perspective. Handbook of reading research, Volume 3, pp. 285-310.

Allport, G. W., 1967. *Readings in attitude theory and measurement.* New York, John Wiley & Sons.

Cox, A., Connolly, S. & Currall, J., 2001. Raising information security awareness in the academic setting. VINE, pp. 11-16.

Furnell, S., Jusoh, A. & Katsabas, D., 2006. The challenges of understanding and using security: a survey of end-users. *Computer Security,* 25(1), pp. 27-35.

Herath, T. & Rao, H. R., 2009. Encouraging information security behaviours in organizations: role of penalties, pressures and perceived effectiveness. *Decision Support System,* 47(2), pp. 154-165.

Krejcie, R. and Morgan, D., 1970, " Determining sample size for research activities", Educational and Psychological Measurement, Vol. 30, pp. 607 - 610.

Kruger, H. & Kearney, W., 2006. A prototype for assessing information security awareness. *Computers & Security,* 25(4), pp. 289-296.

Mccormac, A., Calic, D., Parsons, K., Zwaans, T., Butavicius, M., & Pattinson, M., 2016. Test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q). ACIS 2016 Proceedings. 56.

Mcleod, R. & Schell, J. G., 2008. Management Information Systems. London, Pearson Education.

Microsoft. 1999, Security threats: Best practices for enterprise security [Online]. Available: http://technet.microsoft.com/en-us/library/cc723507.aspx. [Accessed 10 April 2020].

Parsons, K. et al., 2014. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security,* May, Volume 42, pp. 165-176.

Siponen , M., 2001. Five Dimensions of Information Security Awareness. Computers and Society, 31(2), pp. 24-29.

Straub, D., Boudreau, M. & Gefen, D., 2004. Validation guidelines for IS positivist research. *Community Association Information System,* Volume 13, pp. 380-427.

Vroom, C. & Von Solms, R., 2004. Towards information security behavioural

compliance. *Computer Security,* 23(3), pp. 191-198.

Author Biographies

Asanka D. Dharmawansa obtained his PhD and M.Sc. degree in Management and Information systems Engineering from Nagaoka University of Technology, Japan. He obtained his B.Sc. Degree in Industrial Management and computing and Information Systems from the Wayamba University of Sri Lanka. He has published peer-reviewed research articles and reviews in the fields of Information Science, e-Learning and human-computer interaction.

R.A.M. Madhuwanthi obtained her PhD in the Department of Information Science and Control Engineering at Nagaoka University of Technology, Japan. She received her M.Sc. Degree in Operational Research from the Department of Mathematics, University of Moratuwa, Sri Lanka in 2013. She obtained her B.Sc. Degree in Industrial Management and Statistics from Wayamba University of Sri Lanka, Sri Lanka in 2008. Her current research interests include the Information Science, Transportation System Analysis, Safety Management, Cleaner Production and Operational Management.