EMPLOYEES' AWARENESS TOWARDS IT SECURITY MEASURES IMPLEMENTED IN THEIR ORGANIZATION: SELECTED FINANCIAL INSTITUTION

PREMALA NAIR A/P KRISHNAKUTTY

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Science (Information Assurance)

Advanced Informatics School
Universiti Teknologi Malaysia

JUNE 2016

This research is dedicated to my beloved parents, family, friends and colleagues.

ACKNOWLEDGEMENT

This thesis writing wouldn’t be possible without people who have encouraged me throughout the university journey. And this is especially dedicated to my dearest friend J.Moganavatsala who has supported me at all times. Without her I wouldn’t have achieve this dream. I also thank god for giving me the courage, determination and guidance in performing this research despite of the difficulties. I also wish to extend my utmost gratitude to my Project Supervisor Dr. Kamilia Kamardin who has guided me in the whole process of writing this thesis. At last but not least, I would like to thank my superior and colleagues who have covered my duties during my absence on weekends. They have offered me long lasting support and love.

ABSTRACT

This research is aimed to gather the employees’ awareness towards the IT Security measures implemented in their organization case study of a financial institution and from the results gathered can determine the level of IT security awareness among the employees in the organization and suggest security awareness guidelines in order to achieve integrity, availability and confidentiality of the organization. Research on the employees’ awareness towards the IT Security measures implemented in organization is done limitedly in Malaysia. Thus, this research will help to identify current IT security measures implemented, the level of IT security awareness among the employees and how to improve employees’ awareness towards the implementation of the IT security in the organization. Hence, to collect information from the employees sequential explanatory design is used. It is done via quantitative approach then followed by qualitative approach. Thus, both questionnaire and interviews was conducted. Other than that, a literature review also included in order to review the past and current situation, from the review and results pertaining from the data collection and data analysis, security awareness guidelines for the employees is proposed and evaluated.

ABSTRAK

Kajian ini bertujuan untuk mengumpul kesedaran pekerja terhadap langkah-langkah keselamatan teknologi maklumat yang dilaksanakan di dalam organisasi. Kajian kes dibuat di institusi kewangan dan hasil yang dikumpul boleh menentukan tahap kesedaran keselamatan teknologi maklumat di kalangan pekerja di dalam organisasi seterusnya garis panduan untuk melaksanakan tugas dan untuk mencapai integriti, ketersediaan atau kerahsiaan organisasi dapat dicadangkan. Penyelidikan mengenai kesedaran pekerja terhadap beberapa langkah keselamatan teknologi maklumat didalam organisasi dilakukan secara terhad di Malaysia. Kajian ini dapat membantu untuk mengenal pasti langkah-langkah keselamatan teknologi maklumat yang dilaksanakan, tahap kesedaran keselamatan teknologi maklumat di kalangan kakitangan dan cara-cara untuk meningkatkan kesedaran pekerja terhadap pelaksanaan keselamatan teknologi maklumat di organisasi. Oleh itu, bagi mengumpul maklumat daripada pekerja, rekabentuk penjelasan berurutan telah digunakan. Ia dilakukan melalui pendekatan kuantitatif kemudian diikuti oleh pendekatan kualitatif. Seterusnya, soal selidik dan temuduga telah dijalankan. Selain daripada itu, kajian literatur juga telah dibuat untuk mengkaji semula keadaan terdahulu dan juga keadaan semasa. Melalui kajian dan keputusan yang dibuat daripada analisis pengumpulan data, garis panduan kesedaran keselamatan untuk pekerja telah dicadangkan dan dinilai.

TABLES OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

IS	Information Systems
IT	Information Technology
KL	Kuala Lumpur
CCTV	Closed Circuit Television
MitM	Man in the Middle
DoS	Denial of service
DDoS	Distributed Denial of service
ISP	Information Security Policies
ISE	Information Security Education
IST	Information Security Training
SETA	Security Education, Training and Awareness
ISA	Information Security Awareness
TRA/TPB	Theory of Reasoned Action/Theory of Planned Behaviour
GDT	General Deterrence Theory
PMT	Protection Motivation Theory
TAM	Technology Acceptance Model
BI	Behavioural Intention
AB	Actual Behaviour
PSOS	Perceived Severity Of Sanctions
PCOS	Perceived Certainty Of Sanctions
PU	Perceived Usefulness
PEOU	Perceived Ease-Of-Use
ATAM	Architecture Trade-off Assessment
ABAS	Attributes-Based Architecture Styles
ABACUS	Architecture-Based Analysis for Complex Systems
ROA	Real Options Analysis
ISAMM	Information Security Awareness Management Metamodel

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

In any organization, security is the most important aspect. Security can be either physical security, management security or information systems (IS) security. Nowadays, information is also an asset which is as valuable as physical asset in an organization. Thus, all employees should have knowledge on the valuable assets at least at their department level. This will help them in case of emergency they know which is important asset that they need to protect first and which is the asset that considered not that important and they can continue business without that.

Organization need to inform their employee of the security measures which has been implemented in their organization periodically. Employees' must know what type of security measures they have in their department area, in their personal computer or laptop which is provided to them to do their job, and also security measures surrounding them. This is because not all employees have a degree in Information Technology (IT) as such they do not have formal education on the security measures.

1.2 Background of the problem

Security measures in an organization is known as a precaution step taken in combating theft, espionage or sabotage. Thus, organization must implement security measures in order to maintain information integrity and also to minimize risk. Security measures are also important in an organization in maintaining their integrity, availability and confidentiality. Other than that, the policies and regulations of the security measures also allow the organization to maintain, implement, control and audit their security. This will help them in case of any threat or attack to the organization these measures will mitigate the risk and immediately applies the countermeasures.

As such, to protect the organization a security framework can be implemented. The security framework such Spheres of Security can be implemented or use it as a guide to built a quality security measures. This framework is consists of two, where the overview known as “Sphere of Use” while the portion breakdown is known as “Sphere of Protection”. The security measures vary because it depends on the importance of the assets and also on the seriousness or impact of threat that might occur.

On the other hand, the strength of the measures implemented must be determined by the characteristics of the information system and its purposes. As the research done by Tsohoe (2012), the enormous security losses caused by careless behaviour of the employees’ rather than a malicious attack, thus the security awareness play a very important role in inventing a strategic view of information security (Tsohou et al., 2012) .

1.3 Statement of the problem

In the organization, employees mostly use Information Systems on daily basis. Thus employees must ensure that data is protected at all times and it is not lost when a critical situation happens. Mostly the information is stored on the computers in which the information assurance is handled by the IT Security specialists. Unfortunately, employees don’t really know the importance of the Information Security and impact that occurs in case of any emergency.

Thus, this research is done to gather the employees’ awareness towards the IT Security measures implemented in their organization and from the results gathered can determine the level of IT security awareness among the employees in the organization on the security measures and propose to have guidelines to improve employees’ awareness towards the implementation of the IT Security measures in the organization in order to achieve integrity, availability and confidentiality of the organization.

As mentioned by the researcher IT infrastructure which is growing day by day thus it also creates new threats which cannot be predetermined because of that organization faces many security problems where they need to re-evaluate their security measures (Abbas et al., 2011a).

1.4 Research Questions

Research questions are mentioned as below:

i. What IT Security measures are implemented in financial institution: XYZ Bank Bhd?

ii. What is the level of IT security awareness among the employees in the organization?

iii. How to evaluate the proposed guidelines to improve employees' awareness towards the implementation of the IT Security in financial institution: XYZ Bank Bhd?

1.5 Objectives of the Study

The objectives of this study are:

i. To identify current IT Security measures implemented in XYZ Bank Bhd.

ii. To identify level of IT security awareness among the employees in the organization and to propose to have guidelines to improve employees' awareness towards the implementation of the IT Security measures in the organization.

iii. To evaluate the proposed guideline to improve employees' awareness towards the implementation of the IT Security measures in the organization.

1.6 Scope of the Study

The scope of this research covers the following:

i. The research is conducted in XYZ Bank Bhd. XYZ Bank Bhd is a financial institution. It consists of professionals with IT and Non-IT background and medium in size.
ii. Identify the IT Security measures implemented in this organization
iii. To identify level of IT security awareness among the employees in the organization

1.7 Significance of the study

This research is based on the employees in three different branches of XYZ Bank Bhd around Kuala Lumpur area assessing their awareness on IT Security measure implemented in their organization. Other than that, this research also targets to know whether the professionals with IT and Non-IT background are aware on the IT Security measures implemented in their working environment.

Therefore, from this research the theoretical contribution is to identify the IT Security measures implemented in XYZ Bank Bhd and the practical contribution is to measure awareness of the employees' towards the implementation of the IT Security in XYZ Bank Bhd and propose appropriate guideline to enhance their awareness.

REFERENCES

Abbas, H., Magnusson, C., Yngstrom, L., Hemani, A., 2011a. Addressing dynamic issues in information security management. Inf. Manag. Comput. Secur. 19, 5–24. doi:10.1108/09685221111115836

Abbas, H., Magnusson, C., Yngstrom, L., Hemani, A., 2011b. Addressing dynamic issues in information security management. Inf. Manag. Comput. Secur. 19, 5–24. doi:10.1108/09685221111115836

Al-Shawabkeh, M., Saudi, M.M., Alwi, N.H.M., 2012. Computer security self-efficacy effect: An extention of Technology-to-Performance chain model, in: Control and System Graduate Research Colloquium (ICSGRC), 2012 IEEE. IEEE, pp. 64–69.

Amankwa, E., Loock, M., Kritzinger, E., 2014. A conceptual analysis of information security education, information security training and information security awareness definitions, in: Internet Technology and Secured Transactions (ICITST), 2014 9th International Conference for. IEEE, pp. 248–252.

Billingham, S.A., Whitehead, A.L., Julious, S.A., 2013. An audit of sample sizes for pilot and feasibility trials being undertaken in the United Kingdom registered in the United Kingdom Clinical Research Network database. BMC Med. Res. Methodol. 13, 1.

Boyfriend Wilton Mlitwa, N., Birch, D., 2011. The role of intrusion detection systems in electronic information security: From the activity theory perspective. J. Eng. Des. Technol. 9, 296–312. doi:10.1108/17260531111179915

Buck, G., Cook, K., Quigley, C., Eastwood, J., Lucas, Y., 2009. Profiles of Urban, Low SES, African American Girls' Attitudes Toward Science: A Sequential Explanatory Mixed Methods Study. J. Mix. Methods Res. 3, 386–410. doi:10.1177/1558689809341797

Castellan, C.M., 2010. Quantitative and qualitative research: A view for clarity. Int. J. Educ. 2.

Chaturvedi, M., Narain Singh, A., Prasad Gupta, M., Bhattacharya, J., 2014. Analyses of issues of information security in Indian context. Transform. Gov. People Process Policy 8, 374–397. doi:10.1108/TG-07-2013-0019

Dzazali, S., Hussein Zolait, A., 2012. Assessment of information security maturity: An exploration study of Malaysian public service organizations. J. Syst. Inf. Technol. 14, 23–57. doi:10.1108/13287261211221128

Ercan, I., Yazici, B., Sigirli, D., Ediz, B., Kan, I., 2007. Examining Cronbach Alpha, Theta, Omega Reliability Coefficients According to Sample Size. J. Mod. Appl. Stat. Methods 6, 27.

Frangopoulos, E.D., Eloff, M.M., Venter, L.M., 2013. Psychosocial risks: Can their effects on the security of information systems really be ignored? Inf. Manag. Comput. Secur. 21, 53–65. doi:10.1108/09685221311314428

Gao, Y., Peng, Y., Xie, F., Zhao, W., Wang, D., Han, X., Lu, T., Li, Z., 2013. Analysis of security threats and vulnerability for cyber-physical systems, in: Computer Science and Network Technology (ICCSNT), 2013 3rd International Conference on. IEEE, pp. 50–55.

García, M., Llewellyn-Jones, D., Ortin, F., Merabti, M., 2012a. Applying dynamic separation of aspects to distributed systems security: a case study. IET Softw. 6, 231. doi:10.1049/iet-sen.2010.0160

García, M., Llewellyn-Jones, D., Ortin, F., Merabti, M., 2012b. Applying dynamic separation of aspects to distributed systems security: a case study. IET Softw. 6, 231. doi:10.1049/iet-sen.2010.0160

Goldman, E.H., 2012. The effect of acquisition decision making on security posture. Inf. Manag. Comput. Secur. 20, 350–363. doi:10.1108/09685221211286520

Gundu, T., Flowerday, S.V., 2012. The enemy within: A behavioural intention model and an information security awareness process, in: Information Security for South Africa (ISSA), 2012. IEEE, pp. 1–8.

Hall, J.H., Sarkani, S., Mazzuchi, T.A., 2011. Impacts of organizational capabilities in information security. Inf. Manag. Comput. Secur. 19, 155–176. doi:10.1108/09685221111153546

Hazzi, O., Maldaon, I., 2015. A Pilot Study: Vital Methodological Issues. Verslas Teor. Ir Prakt. 16, 53–62. doi:10.3846/btp.2015.437

Jama, A.Y., Siraj, M.M., Kadir, R., 2014. Towards metamodel-based approach for Information Security Awareness Management, in: Biometrics and Security Technologies (ISBAST), 2014 International Symposium on. IEEE, pp. 316–321.

Jankovic, D.Z., 2012. Key security measures for personal data protection in IT systems, in: Telecommunications Forum (TELFOR), 2012 20th. IEEE, pp. 79–82.

Kong, B.S., Kim, M.S., Kim, K.J., 2013a. A Study on Improvement Measures of Unmanned Security System against Security Threats, in: IT Convergence and Security (ICITCS), 2013 International Conference on. IEEE, pp. 1–3.

Kong, B.S., Kim, M.S., Kim, K.J., 2013b. A Study on Improvement Measures of Unmanned Security System against Security Threats, in: IT Convergence and Security (ICITCS), 2013 International Conference on. IEEE, pp. 1–3.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., H. Breitner, M., 2014. Information security awareness and behavior: a theory-based literature review. Manag. Res. Rev. 37, 1049–1092. doi:10.1108/MRR-04-2013-0085

Marett, K., 2015. Checking the manipulation checks in information security research. Inf. Comput. Secur. 23, 20–30. doi:10.1108/ICS-12-2013-0087

Markus Runde, Christopher Tebbe, Karl-Heinz Niemann, 2013. Performance Evaluation of an IT Security Layer in Real-Time Communication. IEEE 1–4.

Mathers, N., Fox, N.J., Hunn, A., 1998. Surveys and questionnaires. NHS Executive, Trent.

Mueller, T., Dittes, S., Ahlemann, F., Urbach, N., Smolnik, S., 2015. Because Everybody is Different: Towards Understanding the Acceptance of Organizational IT Standards. IEEE, pp. 4050–4058. doi:10.1109/HICSS.2015.487

Pallant, J.F., 2004. SPSS survival manual: a step by step guide to data analysis using SPSS. Allen & Unwin, Crows Nest, N.S.W.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., Jerram, C., 2014. A study of information security awareness in Australian government organisations. Inf. Manag. Comput. Secur. 22, 334–345. doi:10.1108/IMCS-10-2013-0078

Peltier, T.R., 2005. Implementing an Information Security Awareness Program. Inf. Syst. Secur. 14, 37–49. doi:10.1201/1086/45241.14.2.20050501/88292.6

Plano Clark, V.L., Huddleston-Casas, C.A., Churchill, S.L., O’Neil Green, D., Garrett, A.L., 2008. Mixed Methods Approaches in Family Science Research. J. Fam. Issues 29, 1543–1566. doi:10.1177/0192513X08318251

Shaaban, H., Conrad, M., 2013a. Democracy, culture and information security: a case study in Zanzibar. Inf. Manag. Comput. Secur. 21, 191–201. doi:10.1108/IMCS-09-2012-0057

Shaaban, H., Conrad, M., 2013b. Democracy, culture and information security: a case study in Zanzibar. Inf. Manag. Comput. Secur. 21, 191–201. doi:10.1108/IMCS-09-2012-0057

Taubenberger, S., Jürjens, J., Yu, Y., Nuseibeh, B., 2013. Resolving vulnerability identification errors using security requirements on business process models. Inf. Manag. Comput. Secur. 21, 202–223. doi:10.1108/IMCS-09-2012-0054

Tavakol, M., Dennick, R., 2011. Making sense of Cronbach’s alpha. Int. J. Med. Educ. 2, 53–55. doi:10.5116/ijme.4dfb.8dfd

Tsohou, A., Karyda, M., Kokolakis, S., Kiountouzis, E., 2012. Analyzing trajectories of information security awareness. Inf. Technol. People 25, 327–352. doi:10.1108/09593841211254358

Wang, P.A., 2010. Information security knowledge and behavior: An adapted model of technology acceptance, in: Education Technology and Computer (ICETC), 2010 2nd International Conference on. IEEE, pp. V2–364.

Zhongping, Z., Kaifeng, Y., yi, Z., Peipei, Z., 2013. Increasing Employees’ Awareness and Enhancing Motivation in E-Government Security Behavior Management. IEEE, pp. 684–687. doi:10.1109/ICDMA.2013.162