A MODEL ON EVALUATING INFORMATION SECURITY AWARENESS IN MAJMAAH UNIVERSITY IN SAUDI RABIA

TALAL NASSER SAUD ALHARBI

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

Faculty of Computing
Universiti Teknologi Malaysia

MAY 2018

This project report is dedicated To My Beloved Parents and my respected supervisor Dr. Maheyzah Md Siraj. to my family for their endless support and encouragement.

ACKNOWLEDGEMENT

First, I would like to thank Almighty ALLAH for giving me the strength and guidance to complete this research project. I also wish to express my sincere thanks and appreciation to my supervisor, Dr. Maheyzah Md Siraj for her support, advice and guidance throughout the completion of this project. With all truthfulness, without ALLAH then her support and motivate, this project would not have been a complete. Dr. Maheyzah Md Siraj has always been source of motivation and guidance. For that, I am truly grateful for her continual support and cooperation in assisting me all the way through my master.

Besides, I would also like to thank my friends, for their continuous helpful guidance and willingness throughout my study. I also like to thank my lovely family for their never-ending love and support through all situations.

Finally, I would like to extend my special gratitude s and thanks to my all lecturers in the Department of Information Security of the Universiti Teknologi Malaysia (UTM) who have given me courage as well their full support during my studies. Last, I would like to thank to my beloved friends members.

ABSTRACT

Evaluating the Information security awareness is consider one of the key and crucial elements of securing information system in organizations. It has been used widely in many fields such as in business, education, marketing, transportation, medical and many other fields. It plays a vital role and thus become challenging issue. Thus security managers should be ready installed and resistance to various numbers of potential attacks. The main reason to fail in many assessment information security awareness is the complexity and inflexibility of the existing models. Domain modulars usually spend many times to understand the nature of the domain, which they desire to model. Even though there are many existing method to evaluate ISA levels appears, but to find best suited way which could provide a straight guideline to ISA users based on their own problems are limited. To solve this limitation, this project follows several steps to create a generic model, which can determine the level of ISA, and its solutions through a unified model. This project addresses the issues of information security awareness towards employees and students in Majmaah University by implementing a conceptual model to support information security awareness for employees and students. The proposed model includes some factors such as; Information security awareness, Education, Bad Experience, Guidelines, Roles and responsibility, Behaviour, Knowledge and Attitude. The model is measured by conducting an online survey to collect data to support the proposed project which results these factors affect on Information Security Awareness by 263 employees and students. The proposed research has contributed to gain a better understanding of evaluating information security awareness to support the Majmaah University by using Cronbach's alpha and regression in the analysis phase. The finding shows the level of information security awareness among students and staff of Majmaah University is moderately aware.

ABSTRAK

Menilai kesedaran keselamatan maklumat adalah salah satu unsur utama dan kritikal untuk melindungi sistem maklumat dalam organisasi. Ia telah digunakan secara meluas dalam pelbagai bidang seperti perniagaan, pendidikan, pemasaran, pengangkutan, perubatan dan banyak bidang lain. Ia memainkan peranan penting dan dengan itu menjadi isu yang mencabar. Oleh itu, pengurus keselamatan perlu dipasang dan menentang pelbagai serangan berpotensi. Adalah penting untuk menentukan apa tindakan balas yang boleh merosakkan organisasi daripada mencapai matlamat perniagaan mereka. Meningkatkan kesedaran kepada tahap yang boleh diterima adalah antara sasaran utama proses pengurusan. Sebab utama gagal dalam menilai kesedaran keselamatan maklumat Kesedaran adalah kerumitan dan ketidakcekapan model-model yang sedia ada. Modul domain biasanya menghabiskan banyak kali untuk memahami sifat domain, yang mereka mahu model. Walaupun terdapat banyak kaedah yang sedia ada untuk menilai tahap ISA, tetapi untuk mencari cara yang paling sesuai yang dapat memberikan panduan lurus kepada pengguna ISA berdasarkan masalah mereka sendiri adalah terbatas. Untuk menyelesaikan masalah ini, projek ini mengikuti beberapa langkah untuk mencipta metamodel generik, yang boleh menentukan tahap ISA, dan penyelesaiannya melalui model bersatu. Projek ini menangani isu kesedaoran kesefamafan maklumat di kalangan pekerja dan pelajar university Majmaah dengan mengimplimen model konsepsi yang menyokong kesedaran keselamatan maklumat di kalangan mereka. Model yang dicadangkan mengandungi factor kesedaran keselamatan, pendidikan pengalaman Buruk, Panduan, Pernan dan tanggungjawab, Tingkahlaku, Pengetahuan dan Sikap. Modelini dinilai dengan kesedaran keselamatan kajiselidik afas talian bagi mengumpul dafa untuk menyokong projek ini di mana ke atasfaktor – factor kesedaran keselamatan maklumana deh 263 pekeja dan pelajar. Penyelidikan yang dicadangkan telah menyumbang kepada pemahaman yang ledih baik terhadap penilaian kesedaran keselamatan maklumat di Universiti Majmaah.

TABLE OF CONTENTS

2 LITERATURE REVIEW

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

ISA	Information Security Awareness
MU	Majmaah University
N	Number of responders
Rho	Pearson's correlation
P	2 tailed
R	Value correlation
R	compare models with their complexity
Beta	coefficients used to determine the magnitude of prediction for each independent variable
T	Test used to determine the significance of predictor
Sig	every one unit increase in the predictor

CHAPTER1 1

INTRODUCTION

1.1 Introduction

The information consider one of the most resources which organizations are very dependent on. If that information of an organization face damage, the organizations could endure difficult problems, that is, in the form of loss of gain, loss of client' trust and probably law action etc. Thus, the information must be secured and protected. Information security awareness is focusing about ensures that all staff are aware about the rules and laws that relative on securing the data inside the organizations. Subsequently, Information security awareness must be a form an integral aspect of each companies' information security management plan.

Mark Wilson and Joan Hash (2003) said awareness is: "Awareness is not just preparing and training. The aims of awareness presentations are to focus interest on security. Awareness presentations are purposed to allow users to recognize IT security necessities and reaction accordingly. In awareness activities, the learner in a training environment has a more active role. much than the learner the recipient of information, Awareness depend on reaching wide audiences or private group with fascinate packaging techniques. Practicing is more normal, also having a goal of building skills and knowledge to assist the job performance."

The European Security Forum Implementation guide (1993), create a definition about information security awareness "the level or extent to which each member of employees comprehensive for the information security importance, the degree of information security appropriate to the organizations, their user security responsibilities, and actions accordingly". In the other side, both of these definitions have some similarity as they both define information security awareness is the level of knowledge and behavior, relating to the information security significance and understanding, and the readiness to behave accordingly.

However, it is too hard to develop the staff's security awareness and change their judgment and behavior for the organization (Wiley, 2009). A lot of organizations have improved and performed several programs in order to enhance and measure their employees‘ awareness about information security. The outcomes for many organizations are unsuccessful programs because the organizations do not practice implement information security. Practice information security in any organization require involvement of employees at all levels. Without that commitment, security techniques may be reduced or pass totally. The aim of the model is to recognize level of ISA based on assessment model at MU.

This chapter presents background on information security, information systems, information security measurement. It also briefly summary the objectives, research problem, aim of the research, contributions, scope, and limitations of this research.

1.2 Problem Background

Majmaah University is one of the emerging Saudi Universities and is receiving interest from the Government. Majmaah University has all the scientific specialties and the newest laboratories in the world and graduated annually from 2000 to 4000 students. The University has more than 3200 employees and approximate 17000 students, so it should be sure all the staff have aware of information security.

The recent years witnessed increasing interest in, new environments for education, and active argumentation, that will shift the emphasis from the traditional model of fixed classroom, involving face-to-face instruction to a flexible model taking into account students' pace and mode (part-time / full time) of learning (Lieberman, et al., 2003). The increased importance of computer systems combined with the availability of the Internet led to the creation of various business applications and services such as Electronic Commerce, Electronic Government, and Online Learning and Education. As a consequence of this universal networking and the extending reach of organization beyond its traditional limit, and with the Internet allowing for a wide variety of undesirable activities, Information Systems Security are considered an important issue (European Security Forum, 1993). Effective IS awareness is becoming one of the most critical factors in protecting information.

The information is now consider as a valuable goods; in fact, the finance world section is almost totally involved in transferring and processing information. However, this worthy commodity is facing threat of attack. The threats of information could be broadly classified as natural disasters e.g. fires, floods, human attacks, or earthquakes e.g. malware threats, other intrusions, hacking, and denial of service attacks (Wiley, 2009). All that risks of natural disasters could be reduced by storing redundant copies of data in several dispersed locations so that will make risks of all copies being damaged or destroyed is incredibly low.

To reduce the incidence and severity of people threats, it is requisite to increase the level of information security awareness inside a specific organization or in the general people. Information security procedures and policies are familiar in many organizations, and seek to give staff clear guidelines on what they could or could not do, thereby increasing the security of companies information, and the general public, is becoming more aware of several threats in information security. However, this is not the situation throughout the countries. In order to measure people awareness, other aspects need be assessed. Kruger and Kearney (2006) suggested that the measurement must address three mains aspects: users' behavior, attitude and knowledge. Based on this study, they have developed a prototype to study the three main questions: what do the user know? How do the user feel? And how do the user behave? Some users might behave in a method that is against their belief or feeling.

1.3 Problem Statement

The reason for computer security violations usually relates to error or misuse apart from malicious activates by the human itself. According to Deanship of Information Technology at Majmaah University, last five years the university has been attacked several times and last attack was from WannCry. Deanship of Information Technology said “that threat happened due to exploitation of lack of awareness among the staff”. There is still no study to identify the level of information security awareness among employees and student.

Heidari (2010) isolated security threats that are specific to social networks. For example, identity blackmailing, theft, online and physical stalking. However, while attempting to mitigate some of these risks, some literature emphasis the importance of awareness in organizations (Adams, 2013). Similarly, there are some techniques for increasing awareness in information technology and communication have been identified (ENISA 2007, Brodie 2009, Heidari 2010, Hinson, 2012), whilst measurement and safety remains a focus of resilience engineering at the safety research scope (Leveson and Hollnagel, 2009).

1.4 Research Questions

How can evaluation will use to measure the information security awareness in Majmaah University?

This purpose of the study is to make a contribution towards awareness effectiveness measurement. The principal problems to be addressed to achieve this purpose could be defined in the form of the following secondary study questions:

1. What are the effect of attitude, knowledge and behavior on staff and students awareness of information security?

2. How to develop a model for evaluating information security awareness in Majmaah University in Saudi Arabia?

3. What is the level of information security awareness in Majmaah University?

1.5 Research Aim

The aim and objective of this study is to determine the level of information security awareness on students' and employees' attitude, behavior, and knowledge by analyzing the result that come from questionnaire. In addition, to measure awareness level of information security Majmaah University.

1.6 Research Objectives

The Objectives of this study also extends to accomplish this following:

1. To identify the effect of attitude, knowledge and behavior on staff and students awareness of information security.
2. To develop a model for evaluating information security awareness in Majmaah University in Saudi Arabia.
3. To measure the level of information security awareness in Majmaah University employees and students.

1.7 Scope Of The Study

The greatest tool to assessment the effectiveness of the organization's security awareness program is a questionnaire. This "Staff Security Awareness Questionnaire" has been designed to claim employees how they can respond to specific security linked survey and status. The survey was distributed among four faculties are Faculty of Engineering, Faculty of Computing, Faculty of Science, and Faculty of Education.

1. The scope of the research focuses on evaluating Awareness of information security in Majmaah University. Also to increase the awareness security.
2. Ten related models have already studied and analyzed. In order to begin and establish a new model. Also, to cover all features and avoid the consequences in information security awareness.

Table 1.1 The ten models, metamodels, and properties.

Authors	Year	Authors	Year
Bilge Karabacaka, Ibrahim	2004	Abdulqader Sheikh Aidaros	2015
L. Drevin, Kruger, Steyn	2007	Ilirjana Veseli	2011
Nurul Hidayah BT AB Rahman	2009	Abdulaziz Saad Al Arifi	2013
Ahmed Yusuf Jama	2014	Robert Poepjes	2015
Mohamed Zulhazmi Bin Khazin	2015	H.A. Krugera, W.D. Kearney	2006

1.8 Significance Of The Research

With this research, it is shown that it is possible for the Majmaah management to proactively measure the effect of awareness efforts on Majmaah Un. Also, the universities management are now aware enough of the prospects of using the evaluate to measure awareness efforts also to secure the information. On the other hand, this study will help the staff in Majmaah University to have aware enough on information security. Also, to make the university choose a right program to rise the aware among staff and students.

Higher education is in a period of historical transition. Many tutors believe that technology can solve many of the current pressures higher education faces, especially those associated with the societal change in attitude and delivery of education (Franklin, et al., 2001). While most if not all information systems security awareness studies have been conducted in developed countries and within a western context; no significant study has been reported in the case of developing countries. This proposed research contributes to the body of knowledge by addressing the identified gaps. The research conducts an exploratory study in IS security awareness within the Majmaah University. Also, the Expected Contribution of the study is: 1- stimulate and best understanding of IS Awareness. 2- reduce of attacks and vulnerabilities faced the university by rising the awareness level through the organization to hold the C.I.A 3- created a successful of modeling to recognize the vulnerabilities to be addressed for Information security awareness.

1.9 Summary

This study is carried out to evolved a model tool which can determine the information security awareness level on Majmaah University so that it could be use to afford input for more effective information security awareness measurement. This chapter determined research problems to recognize the thesis statement and research objectives which led to the research questions. The investigator acknowledged the scientific contribution and the potential challenges of this research. The literature review in this study was also summarised and will be discussed extensively in the next chapter.

REFERENCES

Mark Wilson And Joan Hash. 2003. Building an information technology security awareness and training program‖ computer security division, information technology laboratory, national institute of standards and technology, gaithersburg, md 20899-8933.

European Security Forum. Implementation Guide July 1993: How To Make Your Organisation Aware Of It Security.

David Lacey. Managing The Human Factor In Information Security, Wiley (2009), pp.211

M. Wilson, J. H. October 2003. Building an information technology security awareness and training program. national institute of standards and technology.

ISF. April 2002. Effective Security Awareness (workshop report). Information Security Forum.

Sr., T. P. L. June 2005. Information Security Awareness: The Psychology Behind the Technology. Authorhouse, 1(isbn-13: 978-1420856323).

Division, I. S. July 2008. Security Awareness Program – Strategic Plan Ecommendation (Oregon secretary of state security).

Bill Altermatt. (2007). Internal Consistency Reliability.

System, C. R. 2011. Survey Design (Chapter from the survey system's) http://www.surveysystem.com/sdesign.htm (last visited on 15/11/2017).

Abdullah And Ahmad. (2015). The impact of e-banking on employees job security an empirical study on saudi national banks. International journal of economics, commerce and management.

ENISA. (2009). Information security awareness in financial organisations. available: http://www.enisa.europa.eu/publications/archive/is-in-financial-organisations- 09/at_download/fullreport. Last accessed 30 Sep 2017.

Fadi A. Aloul. (2012). The need for effective information security awareness. Journal of advances in information technology. 3 (.), p176-181

Guillermo Francia, David Thornton, Monica Trifas, Timothy Bowden. (2014). Gamification of information security awareness training. emerging trends in ict security. .(.), 85-95.

Ian Stockwell. (2008). Introduction To Correlation And Regression Analysis. available: http://www2.sas.com/proceedings/forum2008/364-2008.pdf. Last accessed 23th Oct 2017

Mike Marcoe. (N.D). Online security awareness training read more : http://www.ehow.com/facts_7449313_online-security-awareness-training.html. Last accessed 10 nov 2017.

Stefan Bauer, Edward W.N. Bernroider. (2015). The effects of awareness programs on information security in banks: the roles of protection motivation and monitoring. human aspects of information security, privacy, and trust. 9190 (.), 154-164.

Center For Development Of Advanced Computing. Handbook of information security awareness for teacher and parents.

Center For Education And Research In Information Security (cerias). Information security questionnaire: k12 outreach.

Chen, C.C., Shaw, R.S., Yang, S.C. (2006). Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. information technology learning and performance journal.

Drevin, l., Kruger, H.A., Steyn, t. (2007). Value-Focused assessment of ICT security awareness in an academic environment. Computers and security. 26: 36-43.

ISO27001. Code of practice for information security management. UK: British Standards Institute; 2005.

Furnell, S.M., Bryant, P., Phippen, a.d. (2007). Assessing the security perceptions of personal internet users. Computers & security. 26 (5): 410 – 417.

Furnell, S.M., Gennatou, M., Dowland, P.S. (2002). A prototype tool for information security awareness in training. logistics information management. 15 (5 – 6): 352-357.

Hentea, M. (2005). A perspective on achieving information security awareness. issues in informing science & information technology. (2): 169-178.

Kruger, H.A., Kearney, W.D., (2006). A prototype for assessing information security awareness. computers & security. 25 (4): 289-296.

Siponen, M.T. (2001). Five Dimensions Of Security Awareness. Computer and society.

Yacine, R., Mark, A. (2008). Information security awareness term in higher education: an exploratory study. computers & security. 27 (7-8):241 – 253.

Haslina Sahar. (2012). A security awareness model for the establishment of a human firewall in taxation agency. University Technology Malaysia

Ong, l., & Chong, C. (2014). Information Security Awareness: An application of psychological factors--a study in malaysia. in 2014 international conference on computer, communications and information technology (CCIT 2014).

Wulgaert, T. (2005). Security Awareness: Best practices to secure your enterprise. Il, USA: ISACA.

Peng Xiong, (2011). Building a successful information security awareness programme for NLI.

Vorgelegt Von, (2015). Studies On Employees' Information Security Awareness.

Abdulqader Sheikh, (2015). Information Security Awareness model for employees in bank albilad

Lean-Ping Ong, (2015). Awareness of information security risks : An investigation of people aspects (a study in malaysia).

Alwuhayd Muteb (2014). Assessing cloud computing security level of awareness among it and non it students in UTM.

Kostas Papagiannakis, (2011). An overview of the current level of security awareness in greek companies.

Noorlaily Izwana Binti Ibrahim (2012). An anti-malvertising model for university students to increase security awareness.

Nurul Hidayah Bnt Ab Rahman , (2009). A prototype to evaluate information security awareness level for teacher and student in secondary school

Bilge Karabacak, (2004). ISRAM: information security risk analysis method

Drevin, Kruger, Steyn, (2007). A framework for evaluating ICT security awareness.

Ilirjana Veseli (2014). Measuring the impact of information security awareness on social networks through password cracking.

Abdulaziz Saad Al Arifi (2014). Assessing information security risk in Aaudi Arabi.

Aobert Poepjes (2015). The development and evaluation of an information security awareness capability model.

Fadi A. Aloul, (2008). Information security awareness in Uae: A survey paper

Ahmed Yousuf Jama, (2014). Towards metamodel basedapproach for information security awareness management.

Bartlomiej T. Hanus, (2014). The impact of information security awareness on compliance with information security policies: a phishing perspective

Adamu Abdullahi Garba, (2014). Digital forensic readiness framework components for zenith bank nigeria

Mohamed Zul Hazmi Bin Mohamed, (2015). Information security awareness model in social networking for teenagers.

Security Awareness Program Special Interest Group PCI: Security Standards Council, (2014).

Faisal Alotaibi, (2016). A survey of cyber-security awareness in Saudi Arabia.

Ali Farooq, (2015). A taxonomy of perceived information security and privacy threats among it security students.

Rahul Bhasker, Bhushan Kapoor (2009). 259 Computer and Information Security Handbook Copyright 2009 , Morgan Kaufmann Inc. All rights of reproduction in any form reserved. 2009 Information Technology Security Management. California State University: .. 259–268.