FACTORS AFFECTING THE INFORMATION SECURITY AWARENESS IN MALDIVES CUSTOMS SERVICE

IBRAHIM NAAIF

A dissertation 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

MAY 2015

This dissertation is dedicated to my parents and my beloved wife for her endless support and encouragement.

"All that I am and hope to be, I owe to you"

ACKNOWLEDGEMENT

IN THE NAME OF ALLAH, MOST GRACIOUS, MOST COMPASSIONATE, MOST MERCIFUL

First of all, praise is due to almighty Allah subhanahu wa ta'ala who has granted countless blessing, knowledge, and strength that allowed me to accomplish this dissertation.

I submit my highest appreciation to my supervisor Associate Professor Dr. Zuraini Ismail. Without her guidance and encouragement, this dissertation would not have materialized. I cannot thank her enough for her tremendous support, her logical thinking and wide knowledge which has been of great value to me. It was a great privilege and honor to work with her. I also would like to express my sincere gratitude towards Dr. Mohd Shahidan Abdullah who has given me the courage to truly face the challenges encountered during my research.

I submit my sincere gratitude to my parents Late Mohamed Abdullah and Zulfa Adam for their prayers, encouragement and endless love. I am especially grateful for all the support and help from my loving wife Fathimath Hamsha, for cheering me up and providing constant encouragement during the entire process. Not to miss my siblings and my parents-in-law who have also been wonderful and very patient throughout.

Finally, I would like thank all my friends and classmates in University Technology Malaysia for their moral support during my study. To those who indirectly contributed to this research, your kindnesses are highly appreciated.

ABSTRACT

While information security awareness plays a vital role in protecting the organizational information security, it is important to identify the factors affecting information security awareness in order to minimize the threats associated with it. This study aims to identify the factors affecting information security awareness at Maldives Customs Service (MCS). A proposed model was designed and evaluated to identify the factors influencing information security awareness in MCS. A quantitative research was carried out where an online survey was conducted and distributed to operational level staff at MCS. The study results were then analyzed using SPSS v21 and Microsoft Excel 2010. The results show a positive correlation between the identified factors, namely Policy, Behavior, Knowledge and Awareness Governance. Awareness Governance recorded the highest correlation (44%) from the 4 factors. The factors predict 51% of variations on Information Security Awareness (ISA) in Maldives Customs Service. The study may contribute to the development of Information Technology (IT) procedures, awareness programs and policy for managing MCS.

ABSTRAK

Walaupun kesedaran terhadap keselamatan maklumat memainkan peranan penting dalam melindungi keselamatan maklumat organisasi, namun faktor-faktor yang memberi kesan kepada kesedaran keselamatan maklumat perlu dikenalpasti untuk mengurangkan ancaman yang berkaitan. Kajian ini bertujuan untuk mengenal pasti faktor-faktor yang mempengaruhi kesedaran keselamatan maklumat di Perkhidmatan Kastam Maldives (PKM). Model yang dicadangkan telah direka dan dinilai untuk mengenal pasti faktor-faktor yang mempengaruhi kesedaran keselamatan maklumat di PKM. Satu penyelidikan kuantitatif telah dijalankan di mana soal selidik kajian ini telah dijalankan secara dalam talian dan telah diedarkan kepada kakitangan peringkat operasi di PKM. Keputusan kajian dianalisis menggunakan SPSS v21 dan Microsoft Excel 2010. Hasil kajian menunjukkan korelasi positif di antara faktor-faktor yang dikenalpasti, iaitu dasar, kelakuan, pengurusan pengetahuan dan kesedaran. Pengurusan kesedaran direkodkan mempunyai korelasi tertinggi iaitu 44% berbanding empat faktor yang lain. Faktor ini juga meggambarkan 51% variasi Kesedaran Keselamatan Maklumat (KKM) dalam Perkhidamatan Kastam Maldives. Kajian ini boleh menyumbang kepada pembangunan prosedur, program kesedaran dan dasar teknologi maklumat di dalam pengurusan PKM.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

MCS	Maldives Customs Service
ISA	Information Security Awareness
IT	Information Technology

CHAPTER 1

INTRODUCTION

1.1 Overview

With globalization, every organization is dependent on various sources of information data in their daily routine. With the technological advancements today, companies' dependency on information systems and internet has increased vastly focusing mainly on the cyberspace. Information technology is used immensely across an organizational hierarchy for data storage, transmission, recovery and analysis of sensitive data. The need for organizational information security is therefore increasing with one of the main reason being the usage of cyberspace as a main hub for information sharing in-between organizations and institutions. However, an organizations information security breaches cannot be solely blamed on technical faults or the threats associated with. Rather than these, the organization employees must be briefed and made aware on the steps associated with protecting the organizational information.

In a recent study in UK, Figure 1.1 highlighted that the worst security breached in the year 2014 were caused by involuntary human error. The research findings prove that although staff negligence has decreased when compared to the year 2013, it still played a key role in security violations in organizations (Department for Business Innovation and Skills, 2014).

58%	of large organisations suffered staff-related security breaches (down from 73% a year ago)
22%	of small businesses suffered staff-related security breaches (down from 41% a year ago)
31%	of the worst security breaches in the year were caused by inadvertent human error (and a further 20% by deliberate misuse of systems by staff)

Figure 1.1 Security breached by staff (Department for Business Innovation and Skills, 2014)

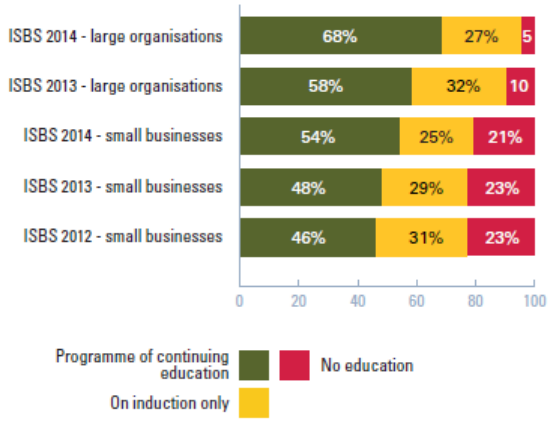

Figure 1.2 How do respondents ensure staff are aware of security threats (Department for Business Innovation and Skills, 2014)

Figure 1.2 illustrates that continuing education is an important factor for larger and smaller enterprises in ensuring staff security awareness. According to the survey 68% of large organizations and 54% of small businesses carry out continuous security training to their employees. More organizations recognize the importance of staff but also those they are a huge risk to the organization which may cause potential damages. The study also determines that the risk associated by employees to larger companies were more than that to the smaller organizations where more risk was originated to them via outside attacks (Department for Business Innovation and Skills, 2014).

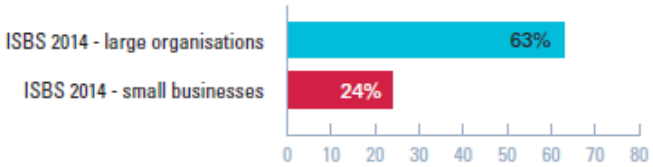

Figure 1.3 How many respondents have staff related incidents (Department for Business Innovation and Skills, 2014)

Figure 1.3 shows the overall staff related incidents are weighed by 63% to larger organizations and 24% to smaller organizations respectively. According to the study, staff associated threats have decreased compared to previous results with more companies having adapted to staff awareness programs. Awareness training programs and behavior are two key factors affecting the overall ISA in an organization. The study justifies that awareness training programs aids to improve employee behavior in minimizing security threats in an organization (Department for Business Innovation and Skills, 2014).

Information technology facilitates a platform for the organization stakeholders and staff to perform more effectively and efficiently. Internet has opened a less time consuming gateway for the organizations. ISA is essential to appropriately protect data from exposure to increasing number of vulnerabilities. *"If security infrastructure is the engine, staff awareness is the oil that makes that engine run"*(Smith, 2006).

This research aims to investigate the key factors affecting ISA in MCS. A model is developed specifically targeted to MCS, which will facilitate MCS to identify the factors affecting ISA in MCS. The model will be evaluated through an online survey using an online questionnaire.

1.2 Background of the Problem

Technological advancement with information communication technology also came with a price, and with it came threats. The popularity in using online methods to carry out critical transactions have lured criminals to exploit weakness which can result in loss of identity, service interruption, legal actions and most importantly loss of money to both business and organization (Khan, Alghathbar, Nabi, & Khan, 2011). Security being a key element of information system plan and design, physical prevention measures alone or by training and creating ISA among the technological staff and management itself are not sufficient (Smith, 2006).

Zaini & Masrek (2013) argues that information security at a general concept is achieved by establishing, implementing and monitoring an appropriate set of control measures which are reviewed and improved where necessary. Whereas, Smith (2006) claims that the companies increasing their investment on the IT infrastructure have however lacked to cater the companies' information security thus increasing the impact of the exposed vulnerabilities. Smith (2006) highlights the importance of overall staff awareness on information security knowledge covering all the levels of the organizational hierarchy.

According Bashorun, Worwui, and Parker (2013), human element is the weakest link in an organizational security protection. Hence it cannot be achieved by only addressing to physical and technical security procedures. Therefore ISA can be described as the knowledge and behavior that the employees of an organization have towards the protection of physical and information assets of the organization.

Information security awareness is a vital factor in protecting the organizational information which is associated with ongoing risks to their systems. Despite the organizations having implemented information security measures, the threats associated to information security are increasing and has reached critical levels. Risk of encountering problems and difficulties are high if the organization

fails to manage their information security systems (Waly, Tassabehji, & Kamala, 2012).

Bashorun, Worwui, and Parker (2013), Waly, Tassabehji, and Kamala (2012) and Smith (2006) have argued that organizations have embraced the idea that the protection of sensitive information by intense technological solutions itself cannot be attained most efficiently. Technology has become the driving force of every aspect of life today and awareness guarantees enterprise staff of their responsibilities assuring the security of the information assets. It is very critical for organizations to adapt to structural information security awareness approach besides their policies and technological controls.

Bashorun, Worwui, and Parker (2013) highlights the importance of ISA to an organization thus providing knowledge and training to all employees rather than focusing to a specific group such as technical staff. This will thus create revolutionized internal change of behavior towards information security awareness in the organization where all employees adapt to good practices in terms of protecting the organization information assets.

1.3 Problem Statement

In addition to the views of different researchers, information security awareness has been proven as an important and essential element to the organization in terms of overcoming various risks that it is being exposed to in a day to day ritual (Bashorun, Worwui, & Parker, 2013; Waly, Tassabehji, & Kamala, 2012; Smith, 2006). Despite the existing policies and procedures regarding information security, many organizations lack awareness among their employees. Some organizations have a briefing session for all new employees at the time of orientation where the employees are made aware on the organization policies. This is not a continuous process meaning that some organizations do not continue further trainings or awareness programs thereafter.

The report published by International Telecommunication union (ITU) (2014) on cyber wellness profile of Maldives states that, Maldives do not follow any information security standards. The limitations on the security standards thus creates a negative impact on MCS in terms of information security and its awareness. A model identifying the factors affecting information security awareness would hence benefit MCS in strengthening the organization information security awareness.

1.4 Research Questions

i. What are the factors affecting information security awareness?
ii. How to design an information security awareness model for MCS?
iii. How to evaluate the proposed information security awareness model for MCS?

1.5 Research Objectives

i. To identify the factors affecting information security awareness
ii. To design an information security awareness model for MCS
iii. To evaluate the proposed information security awareness model for MCS

1.6 Project Aim

The main objective of this study is to investigate the key factors affecting information security awareness in an organization therefore identifying the awareness level of information security among the employees of MCS. Subsequently, the author intends to propose a model consisting of the determined factors affecting information security awareness to MCS. Besides, the author will evaluate effectiveness of proposed ISA model to MCS.

1.7 Scope of the Study

Based on the purpose and objectives of this study, the scope of this research will be as follows:

i. Design an information security awareness model for MCS

ii. The methodology used for this study is quantitative data collection from a sample of 191 respondents by conducting a survey via online questionnaires.

iii. The units of analysis are the employees of MCS

iv. The software used to analyze the survey findings is SPSS v21 and Microsoft excel 2010

1.8 Significance of Study

The theoretical framework of this research identifies the factors affecting ISA in an organization using theories and approaches that are suggested by various researches. Yildirim et.al (2011), Khan et.al (2011), Kamal et.al (2012), Kruger et.al (2006), Olusegun and Ithnin (2013), Siponen and Puhakainen (2010) and Lin et.al (2010) researches are the key theories used in identifying the factors affecting ISA. All these theories were consolidated for designing the model to identify the factors affecting ISA in Maldives Customs Service.

Since there are lack of studies carried out using quantitative techniques towards identifying the factors affecting ISA in Maldives customs service, the methodological contribution of this research aims to provide some information regarding the factors effecting ISA in MCS. A quantitative analysis is conducted via an online questionnaires among operational level employees of MCS.

Information technology facilitates a platform for the organization stakeholders and staff to perform their tasks more effectively. The technological advancement brought with it a number of threats and issues the organizations need to mitigate in order to secure the information. The practical contribution of the research aims to bring a positive impact on MCS by assisting them to understand the importance on how to increase information security awareness, develop policies and schedule training programs in the organization.

1.9 Report organization

The structure of this research is as follows:

Figure 1.4 Report Organization

This research includes five main chapters. Chapter one (1), the introduction of the research begins with the overview of the research followed by research topic, the background of the problem and the problem statement. Chapter two (2) reviews the related studies on the research field. Chapter three (3) describes the research methodology. Chapter four (4) contains the analysis of the study. Chapter five (5) provides the conclusion, recommendations and future work.

1.10 Summary

This chapter provides an overview of the background of the problem in detail. The author has addressed the research objectives and the research questions, furthermore mentioning the statement of the problem. The author has concluded this chapter with the scope, significance of the study and a report organization.

REFERENCES

Abawajy, J., Thatcher, K., & Kim, T. (2008). Investigation of Stakeholders Commitment to Information Security Awareness Programs. *2008 International Conference on Information Security and Assurance (isa 2008)*, 472–476. doi:10.1109/ISA.2008.25

Aggeliki Tsohou, Maria Karyda, Spyros Kokolakis, Evangelos Kiountouzis. 2013. Managing the introduction of information security awareness programmes in organisations. European Journal of Information Systems

Alarifi, A., Tootell, H., & Hyland, P. (2012). A Study of Information Security Awareness and Practices in Saudi Arabia, 6–12.

Arnason, S.T, & Willett, K.D, 2008. How to Archieve 27001 Certification. New York: Auerbach Publications.

Asri, M., Stambul, M., & Razali, R. (2011). An Assessment Model of Information Security Implementation Levels, (July).

Bashorun, A., Worwui, A., & Parker, D. (2013). Information security: To determine its level of awareness in an organization. *2013 7th International Conference on Application of Information and Communication Technologies*, 1–5. doi:10.1109/ICAICT.2013.6722704

Boujettif, M., & Wang, Y. (2010). Constructivist Approach to Information Security Awareness in the Middle East. *2010 International Conference on Broadband, Wireless Computing, Communication and Applications*, 192–199. doi:10.1109/BWCCA.2010.70

Bradley, N. (2010). Marketing Research tools and techniques.

Chalaris, I., Lemos, P.P and Chalaris, M. (2005). IT Governance: The Safe Way to Effective and Efficient Governance. *E-Journal of science and Technology*. Vol. 1, Issue 1, pp. 59-63. ISSN 17905613.

Coakes, S.J., Steed, L., & Ong, C. (2009). SPSS 16.0 for windows: Analysis without anguish. Australia: John Wiley and Sons.

Cohen, L., Manion, L., & Morrison, K. (2007). *Research Methods in Education*.

Costello, a, & Osborne, J. (2005). Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis. Practical Assessment, Research & Evaluation, 10(7), 1–9.

DeCoster, J. (2004). Data Analysis in SPSS. Retrieved <April-25- 2015> from http://www.stat-help.com/notes.html

De Haes, S., & Grembergen, W. Van. (2006). Information Technology Governance Best Practices in Belgian Organizations, 1–15. Retrieved from internal-pdf:/IT Governance Best Practices in Belgian Organizations.pdf

Department for Bussiness Innovation and Skills (2014) Information Security Breaches Survey, UK: Department for Bussiness Innovation and Skills. Available at http://www.pwc.co.uk/assets/pdf/cyber-security-2014-exec-summary.pdf

De Vaus, D. A. (2002). Survey in Social Research (5th Edition). Psychology Press

De Winter, J. C. F., Dodou, D., & Wieringa, P. a. (2009). Exploratory Factor Analysis With Small Sample Sizes. Multivariate Behavioral Research, 44(2), 147–181. doi:10.1080/00273170902794206

Dhillon G, Backhouse J. (2000). Information system security management in the new millennium. *Communications of the ACM*; 43(7):125–8

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *4*(April), 92–100. Retrieved from 10.4236/jis.2013.42011\nhttp://search.ebscohost.com/login.aspx?direct=true&db=i3h&AN=89254050&site=ehost-live

ESOMAR (2013) Industry Report 2013, : On Device Research. Available at https://ondeviceresearch.com/blog/esomar-2013-industry-report-weather-forecast-for-mobile

Evaluation, E. (2008). Data Collection Methods for Program Evaluation: Questionnaires, *15*(14).

Faisal, A. A., & Ibrahim, J. (2013). Mitigating privacy issues on Facebook by implementing information security awareness with islamic perspectives. *2013 5th International Conference on Information and Communication Technology for the Muslim World (ICT4M)*, 1–5. doi:10.1109/ICT4M.2013.6518896

Field, A. P. (2005). Discovering Statistics Using SPSS (2nd Edition). London: Sage.

Gantz, B. J., & Reinsel, D. (2011). Extracting Value from Chaos State of the Universe : An Executive Summary, (June), 1–12.

George, D., & Mallery, P. (2003). SPSS for Windows step by step: A simple guide and reference. 11.0 update (4th ed.). Boston: Allyn & Bacon.

Gliem, J. a, & Gliem, R. R. (2003). Calculating, Interpreting, and Reporting Cronbach's Alpha Reliability Coefficient for Likert-Type Scales,. 2003 Midwest Research to Practice Conference in Adult, Continuing, and Community Education, (1992), 82–88. doi:10.1109/PROC.1975.9792

Gundu, T., & Flowerday, S. V. (2013). Ignorance to awareness: Towards an information security awareness process. *SAIEE Africa Research Journal*, *104*(2), 69–79.

Hardy, G. (2002). Make Sure Management and IT are on the Same Page: Implementing an IT Governance Framework. *The Information System Control Journal*. Vol. 3.

Henson RK, Roberts JK. (2006) Use of Exploratory Factor Analysis in Published Research: Common Errors and Some Comment on Improved Practice. Educational and Psychological Measurement.

International Telecommunication Union (2014) Cyberwellness Profile Maldives, : International Telecommunication Union (ITU). Available at www.itu.int/en/ITU-D/Cybersecurity/Documents/...Profiles/Maldives.pdf

ISO/IEC. Information technology – code of practice for information security management, ISO/IEC 27002:2005. The International Organization for Standardization/The International Electrotechnical Commission; 2005.

ITGI (2003). Board Briefing on IT Governance. 2nd Edition. IT Governance Institute. Available at http://www.itgi.org

Jain, A. K., Ross, A., Pankanti, S., & Member, S. (2006). Biometrics : A Tool for Information Security, *1*(2), 125–143.

James P. Stevens. (2002). Applied Multivariate Statistics For The Social Sciences (4th Edition). London: Lawrence Erlbaum Associates, Publishers.

Johnson, E.C. (2005). IT Governance: New PLayers, Challenges and Opportunities. *The information systems control journal.* Vol. 2.

Joseph F. Hair, William C. Black, Barry J. Babin, Rolph E. Anderson (2009). Multivariate Data Analysis (7th Edition). New Jersey: Prentice-Hall.

Kamal, S., Fakeh, W., Zulhemay, M. N., Shahibi, M. S., & Ali, J. (2012). Information Security Awareness Amongst Academic Librarians, *8*(3), 1723–1735.

Kankanhalli A, Teo HK, Tan BCY, Wei KK. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*;23:139–54.

Kaur, J., & Mustafa, N., (2013) Examining the Effects of Knowledge, Attitude and Behaviour on Information Security Awareness: A Case on SME. *3rd*

International Conference on Research and Innovation in Information Systems, 286-290

Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, *5*(26), 10862–10868. doi:10.5897/AJBM11.067

Knapp, K. J., Franklin Morris, R., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security*, *28*(7), 493–508. doi:10.1016/j.cose.2009.07.001

Kruger, H. a., Flowerday, S., Drevin, L., & Steyn, T. (2011). An assessment of the role of cultural factors in information security awareness.

Kruger, H. a., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289–296. doi:10.1016/j.cose.2006.02.008

La Corte, A., & Scatà, M. (2010). A process approach to manage the security of the communication systems with risk analysis based on epidemiological model. *Proceedings - 5th International Conference on Systems and Networks Communications, ICSNC 2010*, 166–171. doi:10.1109/ICSNC.2010.32

Levin M, Klev R (2002). Forandring som praksis : læring og utvikling i organisasjoner. In Norwegian [Changes in practice: learning and development in organizations] Bergen, Fagbokforlaget

Lewis, A. (2000). Time to elevate IT security to the boardroom, e Secure, 1(1): 28

Lin, Y. M., Arshad, N. H., Haron, H., Yusoff, M., Wah, Y. B., & Mohammed, A. (2010). IT Governance Awareness and Practices : an Insight from Malaysian Senior Management Perspective, *5*(1), 43–57.

Linden, A. (2013). The importance of technology management in the ICT requirements definition process. *Technology Management in the IT-Driven Services (PICMET), 2013 Proceedings of PICMET '13:*, 2283–2295.

Luftman, J.N., Bullen, C.V., Liao, D., Nash, E., & Neuman, C. (2004). *Managing the information Technology Resource: Leadership in the information Age.* Pearson Prentice Hall, Inc.

Maldives Customs Service. 2014. Maldives Customs Service - History. [ONLINE] Available at: http://www.customs.gov.mv/organization/history. [Accessed 19 November 14].

Maldives Customs Service. 2014. Maldives Customs Service - Vison and Misson. [ONLINE] Available at: http://www.customs.gov.mv/organization/vision_mission. [Accessed 19 November 14].

Malta Information technology Agency [poster] Available At: ttps://www.mita.gov.mt/en/Security/SecurityAwareness/PublishingImages/1_ClearDeskandClearScreen_web.jpg [Accessed on 23.11.2014]

Mcleod, R., and Schell, J. G. (2008). Management Information Systems. London: Pearson Education

Momeni, A., & Ph, R. (2009). Information Management And The Role Of Information And Knowledge Managers : Managers ' Perception, (July), 2504–2516.

Namjoo, Dan, Jahyun, & Andy. (2008). Knowing is Doing: An Emperical Validation Of the Relationship between Managerial Information Security Awareness and Action.

National Institute of Standards and Technology (2000). An Introduction to Computer Security: The NIST Handbook., Special Publication 800-12. United States Dept. of Commerce, Technology Administration, National Institute of Standards and technology, United States.

National Institute of Standards and Technology Special Publication (2006), 800-53, Revision 1, Recommended Security Controls for Federal Information System,

Newbould, M., & Furnell, S. (2009). Playing Safe : A Prototype Game For Raising Awareness of Social Engineering, (December).

O'Leary, Z. (2004). The Essential Guide to Doing Research.

Olusegun, O. J., & Ithnin, N. B. (2013). " People Are the Answer to Security ":, *11*(8).

Payton, M. E., Greenstone, M. H., & Schenker, N. (2003). Overlapping confidence intervals or standard error intervals: What do they mean in terms of statistical significance? *Journal of Insect Science*, 3, 34.

Pett, M. A., N. R. Lackey, et al. (2003). Making Sense of Factor Analysis: The use of factor analysis for instrument development in health care research. California, Sage Publications Inc.

Phellas, C. N., Bloch, A., & Seale, C. (2011). Structured Methods : Interviews , Questionnaires And Observation, 181–205.

Raees, K. (2010). Practical Approaches to Organizational Information Security Management.

Read, T.J., (2004) Discussion of Director Responsibility for IT Governance: A Perspective on Strategy. *International Journal of Accounting Information Systems.* Vol.5, pp.105-107. 2004 Elsevier Inc.

Robinson, A. (2013). Using Influence Strategies to Improve Security Awareness Programs.

Salman, A. (2005). Organization Needs and Everyone's Responsibility- Information Security Awareness. *SANS Institute*.

Sapnas, K. G. and R. A. Zeller (2002). "Minimizing sample size when using exploratory factor analysis for measurement." Journal of Nursing Measurement. 10(2): 135-153.

Schönrock-Adema, J., Heijne-Penninga, M., van Hell, E. A., & Cohen-Schotanus, J. (2009). Necessary steps in factor analysis: enhancing validation studies of educational instruments: The PHEEM applied to clerks as an example. Medical Teacher, 31(6), 226-232.

Sharma, D., Mcgee, D., & Kibria, B. M. G. (2011). Measures of Explained Variation and the Base-Rate Problem for Logistic Regression, 2(1), 11–19.

Shaw, R., Chen, C., Harris, A. and Huang, H. (2008). The impact of information richness on information security awareness training effectiveness. Computers and Education, 52(2), 92-100.

Shuchih Ernest Chang, Chienta Bruce Ho, (2006) "Organizational factors to the effectiveness of implementing information security management", Industrial Management & Data Systems, Vol. 106 Iss: 3, pp.345 - 361

Siponen, M., & Puhakainen, P. (2010). Improving E Mployees ' C Ompliance T Hrough I Nformation S Ystems S Ecurity T Raining :, *34*(4), 757–778.

Siponen, M. T. (2008). A conceptual foundation for organizational information security awareness A conceptual foundation for organizational information security awareness.

Smith, M. (2006). The Importance of Employee Awareness to Information Security. *Crime and Security, 2006. The Institution of Engineering and Technology Conference on*, 115–128.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information Security Management System Standards : A Comparative Study of the Big Five, (October).

Tabachnick BG, Fidell LS. (2007). Using Multivariate Statistics. Boston: Pearson Education Inc

Takemura, T. (2010). A Quantitative Study on Japanese Workers ' Awareness to Information Security Using the Data Collected by Web-Based Survey Toshihiko Takemura, *2*(1), 20–26.

Talib, S., Clarke, N. L., & Furnell, S. M. (2010). An Analysis of Information Security Awareness within Home and Work Environments. *Availability, Reliability, and Security, 2010. ARES '10 International Conference on*, 196–203. doi:10.1109/ARES.2010.27

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. International Journal of Medical Education, 2, 53–55. doi:10.5116/ijme.4dfb.8dfd

Thompson B. (2004) Exploratory and confirmatory factor analysis: understanding concepts and applications. Washington, DC: American Psychological Association.

Von Solms, R. & Von Solms, S. H. (2004a). From policies to culture. Computers & Security, 23(4): 275-279

Waint, T.L. (2005). Information security policy's impact on reporting security incidents, Computers & Security, 24(6): 448-459

Waly, N., Tassabehji, R., & Kamala, M. (2012). Improving Organisational Information Security Management: The Impact of Training and Awareness. *2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems*, 1270–1275. doi:10.1109/HPCC.2012.187

Williams, B., Brown, T., & Onsman, A. (2012). Exploratory factor analysis : A five-step guide for novices. Journal of Emergency Primary Health Care (JEPHC), 8(3), 1–13.

Yeniman Yildirim, E., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management*, *31*(4), 360–365. doi:10.1016/j.ijinfomgt.2010.10.006

Yoshioka, N., Washizaki, H., & Maruyama, K. (2008). A survey on security patterns. Progress in Informatics, 5(5), 35-47.

Zaini, M. K., & Masrek, M. N. (2013). Conceptualizing the Relationships between Information Security Management Practices and Organizational Agility. *2013 International Conference on Advanced Computer Science Applications and Technologies*, 269–273. doi:10.1109/ACSAT.2013.60