Bibliography

Abdallah, S., & Fan, I. S. (2012). Framework for e–government assessment in developing countries: case study from Sudan. *Electronic Government, an International Journal, 9*(2), 158-177.

Abramson, M. A., & Means, G. (2001). E-government 2001, The Price water house Coopers endowment series on the business of government: Lanham, Md.: Rowman & Littlefield.

Abu-Musa, A. (2010). Information security governance in Saudi organizations: an empirical study. *Information Management & Computer Security, 18*(4), 226-276.

Adams, J., Khan, H. T., & Raeside, R. (2014). *Research methods for business and social science students*: SAGE Publications India.

Adams, J., Khan, H. T., Raeside, R., & White, D. I. (2007). *Research methods for graduate business and social science students*: SAGE Publications India.

Akhgar, B., & Arabnia, H. R. (2013). *Emerging trends in ICT security*: Newnes.

Al-Ahmad, W., & Al-Kaabi, R. (2008). *An extended security framework for e-government.* Paper presented at the Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference on.

Al-Awadi, M., & Renaud, K. (2007). *Success factors in information security implementation in organizations.* Paper presented at the IADIS International Conference e-Society.

Al-Azri, A., Al-Salti, Z., & Al-Karaghouli, W. (2010). The successful implementation of e-government transformation: a case study in Oman.

Al-Hashmi, A., & Darem, A. B. (2008). Understanding phases of E-government project. *New Delhi: Retrieved from http://www.csi-sigegov. org/emerging_pdf/17_152-157. pdf.*

Al-Khouri, A. M., Farmer, M., & Qadri, J. (2014). A government framework to address identity, trust and security in egovernment: The Case of UAE Identity Management Infrastructure. *European Scientific Journal, 10*(10).

Al-Omari, A., Deokar, A., El-Gayar, O., Walters, J., & Aleassa, H. (2013). *Information Security Policy Compliance: An Empirical Study of Ethical Ideology.* Paper presented at the System Sciences (HICSS), 2013 46th Hawaii International Conference on.

Al-Salihy, W., Ann, J., & Sures, R. (2003). *Effectiveness of information systems security in IT organizations in Malaysia.* Paper presented at the Communications, 2003. APCC 2003. The 9th Asia-Pacific Conference on.

Al-Shafi, S., & Weerakkody, V. (2010). Factors affecting e-government adoption in the state of Qatar.

Al-Tameem, A., Zairi, M., & Kamala, M. (2009). *Critical factors of information security implementation.* Paper presented at the Networked Digital Technologies, 2009. NDT'09. First International Conference on.

Aladwani, A. M. (2016). Corruption as a source of e-Government projects failure in developing countries: A theoretical exposition. *International Journal of Information Management, 36*(1), 105-112.

Alfawaz, S., May, L. J., & Mohannak, K. (2008). E-government security in developing countries: A managerial conceptual framework.

Alfawaz, S., Nelson, K., & Mohannak, K. (2010). *Information security culture: a behaviour compliance conceptual framework.* Paper presented at the Proceedings of the Eighth Australasian Conference on Information Security-Volume 105.

Alfawaz, S. M. (2011). *Information security management: a case study of an information security culture.* Queensland University of Technology.

AlHogail, A., & Mirza, A. (2014). *Information security culture: a definition and a literature review.* Paper presented at the Computer Applications and Information Systems (WCCAIS), 2014 World Congress on.

Aliti, A., & Akkaya, D. (2011). Employees' Role in Improving Information Systems Security.

AlKalbani, A., Deng, H., & Kam, B. (2014). *A Conceptual Framework for Information Security in Public Organizations for E-Government Development.*

AlKalbani, A., Deng, H., & Kam, B. (2015). *Organisational security culture and information security compliance for e-government development: the moderating effect of social pressure.* Paper presented at the PACIS 2015.

Allison, P. D. (2012). *Handling missing data by maximum likelihood.* Paper presented at the SAS global forum.

Almarabeh, T., & AbuAli, A. (2010). A general framework for e-government: definition maturity challenges, opportunities, and success. *European Journal of Scientific Research, 39*(1), 29-42.

Alnatheer, M., & Nelson, K. (2009). Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context.

Alnatheer, M. A. (2012). Understanding and measuring information security culture in developing countries: case of Saudi Arabia.

Alnatheer, M. A. (2014). A Conceptual Model to Understand Information Security Culture. *International Journal of Social Science and Humanity, Vol. 4, No. 2.*

Alnatheer, M. A. (2015). *Information Security Culture Critical Success Factors.* Paper presented at the Information Technology-New Generations (ITNG), 2015 12th International Conference on.

Alshboul, R. (2012). Security and Vulnerability in the E-Government Society. *Contemporary Engineering Sciences, 5*(5), 215-226.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological bulletin, 103*(3), 411.

Ashaye, O. O. R., & Irani, Z. (2012). *E-Government Implementation Factors: A Conceptual Framework.* Paper presented at the World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education.

Awang, Z. (2015). SEM Made Simple: A Gentle Approach to Learning Structural Equation Modeling.

Ayyagari, R., & Tyks, J. (2012). Disaster at a University: A Case Study in Information Security. *Journal of Information Technology Education, 11*.

Babbie, E. (2010). The Practice of Social Research.

Bagozzi, R. P. (1980). *Causal models in marketing*: Wiley New York.

Baker, G. (2013). The Government is Now Closed. . .in More Ways Than One. Retrieved from http://www.foreffectivegov.org/blog/opengov-shutdown/

Bandara, W. (2007). Process modelling success factors and measures.

Barton, K. A. (2014). Information System Security Commitment: A Study of External Influences on Senior Management.

Beautement, A., Sasse, M. A., & Wonham, M. (2009). *The compliance budget: managing security behaviour in organisations*. Paper presented at the Proceedings of the 2008 workshop on New security paradigms.

Beavers, A. S., Lounsbury, J. W., Richards, J. K., Huck, S. W., Skolits, G. J., & Esquivel, S. L. (2013). Practical considerations for using exploratory factor analysis in educational research. *Practical assessment, research & evaluation, 18*(6), 1-13.

Belanger, F., & Hiller, J. S. (2006). A framework for e-government: privacy implications. *Business process management journal, 12*(1), 48-60.

Berry, L. M., & Houston, J. P. (1993). *Psychology at work*: WCB/McGraw-Hill.

Best Management Practice. (2007). *An Introductory Overview of ITIL V3*. Retrieved from http://www.best-management-practice.com/gempdf/itSMF_An_Introductory_Overview_of_ITIL_V3.pdf

Biolchini, J., Mian, P. G., Natali, A. C. C., & Travassos, G. H. (2005). Systematic review in software engineering. *System Engineering and Computer Science Department COPPE/UFRJ, Technical Report ES, 679*(05).

Bluhm, D. J., Harman, W., Lee, T. W., & Mitchell, T. R. (2011). Qualitative research in management: a decade of progress. *Journal of Management Studies, 48*(8), 1866-1891.

Brady, J. W. (2011). *Securing health care: Assessing factors that affect HIPAA security compliance in academic medical centers.* Paper presented at the System Sciences (HICSS), 2011 44th Hawaii International Conference on.

Breaux, T. D., & Baumer, D. L. (2011). Legally "reasonable" security requirements: A 10-year FTC retrospective. *Computers & Security, 30*(4), 178-193.

Brodie, C. (2008). The importance of security awareness training.

Brown, T. A. (2015). *Confirmatory factor analysis for applied research*.

Bryman, A. (2012). *Social Research Methods*: Oxford University Press.

Byrne, B. M. (2013). *Structural equation modeling with AMOS: Basic concepts, applications, and programming*: Routledge.

Carsrud, A., & Brännback, M. (2014). *Handbook of Research Methods and Applications in Entrepreneurship and Small Business*: Edward Elgar Publishing, Incorporated.

Castro-Costa, É., Dewey, M. E., Uchôa, E., Firmo, J. O., Lima-Costa, M. F., & Stewart, R. (2014). Construct validity of the mini mental state examination across time in a sample with low-education levels: 10-year follow-up of the Bambuí Cohort Study of Ageing. *International journal of geriatric psychiatry, 29*(12), 1294-1303.

Chan, H., & Mubarak, S. (2012). Significance of information security awareness in the higher education sector. *International Journal of Computer Applications, 60*(10).

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems, 106*(3), 345-361.

Chang, S. E., & Lin, C.-S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*(3), 438-458.

Chaula, J. A. (2006). A Socio-Technical Analysis of Information Systems Security Assurance: A Case Study for Effective Assurance.

Checkland, P., & Scholes, J. (1990). Soft Systems Methodology. Retrieved from http://www.jespersimonsen.dk/Downloads/SSM-IntroductionJS.pdf

Chen, B. (2014). Home Depot investigates a possible credit card breach. *The New York Times*.

Chen, C. C., Dawn Medlin, B., & Shaw, R. (2008). A cross-cultural investigation of situational information security awareness programs. *Information Management & Computer Security, 16*(4), 360-376.

Chen, H., & Li, W. (2014). UNDERSTANDING ORGANIZATION EMPLOYEES INFORMATION SECURITY OMISSION BEHAVIOR: AN INTEGRATED MODEL OF SOCIAL NORM AND DETERRENCE.

Chetty, J., & Coetzee, M. (2010). *Towards an information security framework for service-oriented architecture.* Paper presented at the Information Security for South Africa (ISSA), 2010.

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*(8), 719-731.

Churchill, G. (1999). Marketing research: methodological foundations. *The Dryden Press series in marketing Show all parts in this series.*

Cohen, L., Manion, L., & Morrison, K. (2013). *Research methods in education*: Routledge.

Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days? *Information security technical report, 14*(4), 186-196.

Coopers, P. (2016). *Key findings from the Global State of Information Security Survey 2016.* Retrieved from https://www.pwc.fi/fi/julkaisut/tiedostot/global-state-of-information-security-survey-2016.pdf

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches*: Sage publications.

Cronbach, L. J. (1971). Test validation. *Educational measurement, 2*, 443-507.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *computers & security, 32*, 90-101.

CyberSecurity Malaysia. (2015). Retrieved from https://www.mycert.org.my/en/services/advisories/mycert/2015/main/detail/1100/index.html

D'Arcy, J., & Greene, G. (2009). *The multifaceted nature of security culture and its influence on end user behavior.* Paper presented at the International Workshop on Information Systems Security Research.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research, 20*(1), 79-98.

D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of business ethics, 89*(1), 59-71.

Da Veiga, A. (2015). *The Influence of Information Security Policies on Information Security Culture: Illustrated through a Case Study.* Paper presented at the Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015).

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29*(2), 196-207.

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security, 49*, 162-176.

Da Veiga, A., & Martins, N. (2015). An Information Security Culture Model Validated with Structural Equation Modelling.

Da Veiga, A., Martins, N., & Eloff, J. H. (2007). Information security culture-validation of an assessment instrument. *Southern African Business Review, 11*(1), 147-166.

Deloitte, & Touche. (2001). The citizen as customer. *CMA Management, 74*(10), 58.

Denzin, N. K., & Lincoln, Y. S. (2008). *Strategies of qualitative inquiry* (Vol. 2): Sage.

DeVellis, R. F. (2012). *Scale development: Theory and applications* (Vol. 26): Sage publications.

Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM, 43*(7), 125-128.

Dhillon, G., Tejay, G., & Hong, W. (2007). *Identifying governance dimensions to evaluate information systems security in organizations.* Paper presented at the System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on.

Dimitrov, D. M. (2014). *Statistical methods for validation of assessment scale data in counseling and related fields*: John Wiley & Sons.

DiStefano, C., & Hess, B. (2005). Using confirmatory factor analysis for construct validation: An empirical review. *Journal of Psychoeducational Assessment, 23*(3), 225-241.

Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2007). Fostering information security culture in small and medium size enterprises: an interpretive study in Australia.

Duarte, P. A. O., & Raposo, M. L. B. (2010). A PLS model to study brand preference: An application to the mobile phone market *Handbook of partial least squares* (pp. 449-485): Springer.

Dzazali, S., & Hussein Zolait, A. (2012). Assessment of information security maturity: an exploration study of Malaysian public service organizations. *Journal of Systems and Information Technology, 14*(1), 23-57.

El-Haddadeh, R., Tsohou, A., & Karyda, M. (2012). Implementation challenges for information security awareness initiatives in e-government.

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of advanced nursing, 62*(1), 107-115.

Eloff, J., & Eloff, M. (2005). Information security architecture. *Computer Fraud & Security, 2005*(11), 10-16.

Field, A. (2009). *Discovering statistics using SPSS*: Sage publications.

Field, A. (2013). *Discovering statistics using IBM SPSS statistics*: Sage.

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *computers & security, 43*, 90-110.

Flowerday, S., & Von Solms, R. (2006). Trust: An element of information security *Security and Privacy in Dynamic Environments* (pp. 87-98): Springer.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, 39-50.

Fulford, H., & Doherty, N. F. (2003). The application of information security policies in large UK-based organizations: an exploratory investigation. *Information Management & Computer Security, 11*(3), 106-114.

Furnell, S. M., Clarke, N., Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security, 17*(1), 4-19.

Garson, G. (2012). Testing Statistical Assumption, Blue Book series: Statistical Associates Publishing.

Garson, G. D. (2009). Structural equation modeling. *Statnotes: Topics in multivariate analysis*.

Garson, G. D. (2013). *Factor analysis*.

Gebba, T. R., & Zakaria, M. R. (2012). E-government in Egypt: an analysis of practices and challenges. *International Journal of Technology and Management (IJTM), 1*(1).

Gerring, J. (2011). *Social science methodology: A unified framework*: Cambridge University Press.

Ghasemi, A., & Zahediasl, S. (2012). Normality tests for statistical analysis: a guide for non-statisticians. *International journal of endocrinology and metabolism, 10*(2), 486-489.

Gil-García, J. R., & Pardo, T. A. (2005). E-government success factors: Mapping practical tools to theoretical foundations. *Government Information Quarterly, 22*(2), 187-216.

GORSUCH, R. (2014). Factor analysis. Classic Edition: New York: Routledge.

Grace, J. B., Schoolmaster, D. R., Guntenspergen, G. R., Little, A. M., Mitchell, B. R., Miller, K. M., & Schweiger, E. W. (2012). Guidelines for a graph-theoretic implementation of structural equation modeling. *Ecosphere, 3*(8), 1-44.

Greene, G., & D'Arcy, J. (2010). *Assessing the impact of security culture and the employee-organization relationship on IS security compliance.* Paper presented at the 5th annual symposium on information assurance (ASIA'10).

Gregor, S., & Hevner, A. R. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *MIS quarterly, 37*(2), 337-355.

Guba, E. G., & Lincoln, Y. S. (2005). Paradigmatic Controversies, Contradictions, and Emerging Confluences.

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. *Information management & computer security, 13*(4), 297-310.

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security, 16*(4), 377-397.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2010). *Multivariate data analysis* (Vol. 6): Prentice Hall, Upper Saddle River, New Jersey.

Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2013). *A primer on partial least squares structural equation modeling (PLS-SEM)*: Sage Publications.

Halit, A. H. (2014). THE VALIDITY AND RELIABILITY TEST FOR CAREER INTERVENTION PROGRAM QUESTIONNAIRE (CIPQ).

Hall, J. H., Sarkani, S., & Mazzuchi, T. A. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security, 19*(3), 155-176.

Hall, R. (2012). Mixed methods: In search of a paradigm. *Innovative Research in a changing and challenging world. Australian Multicultural Interaction Institute, Tasmania. http://www. auamii. com/ proceedings_ Phuket_.*

Harris, K. D., General, A., & Lookout, A. (2014). Cybersecurity in the Golden State: California: Department of Justice.

Hartas, D. (2015). *Educational research and inquiry: Qualitative and quantitative approaches*: Bloomsbury Publishing.

Harwell, M. R. (2011). Research design in qualitative/quantitative/mixed methods. *CONRAD, Clifton F.; SERLIN, Ronald C. The SAGE Handbook for Research in Education: Pursuing ideas as the keystone of exemplary inquiry. 2ª Edition. Thousand Oaks, CA: SAGE Publications*, 147-163.

Hassan, N. H., & Ismail, Z. (2012). A conceptual model for investigating factors influencing information security culture in healthcare environment. *Procedia-Social and Behavioral Sciences, 65*, 1007-1012.

Heeks, R. (2003). *Most eGovernment-for-development projects fail: how can risks be reduced?* : Institute for Development Policy and Management, University of Manchester Manchester.

Heeks, R. (2005). *Implementing and managing eGovernment: an international text*: Sage.

Heeks, R., & Bailur, S. (2007). Analyzing e-government research: Perspectives, philosophies, theories, methods, and practice. *Government information quarterly, 24*(2), 243-265.

Hellriegel, D., SLOcUM, J., & Woodman, R. (1998). Organizational behavior, cincinnati. *Ohio, South+ Western college Publ.*

Helokunnas, T., & Kuusisto, R. (2003). *Information security culture in a value net.* Paper presented at the Engineering Management Conference, 2003. IEMC'03. Managing Technologically Driven Organizations: The Human Side of Innovation and Change.

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

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28* (1, March 2004), 75-105.

Hiller, J. S., & Belanger, F. (2001). Privacy strategies for electronic government. *E-government, 200*, 162-198.

HKSAR. (2008). AN OVERVIEW OF INFORMATION SECURITY STANDARDS. *The Government of the Hong Kong Special Administrative Region*. Retrieved from http://www.infosec.gov.hk/english/technical/files/overview.pdf

Howard, M. (2001). E-government across the globe: how will'e'change government. *e-Government, 90*, 80.

Hoyle, R. H. (2011). *Structural Equation Modeling for Social and Personality Psychology*: Sage.

Hoyle, R. H. (2012). *Handbook of structural equation modeling*: Guilford Press.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: the critical role of top management and organizational culture*. *Decision Sciences, 43*(4), 615-660.

Huang, C.-C., & Farn, K.-J. (2016). A Study on E-Taiwan Promotion Information Security Governance Programs with E-government Implementation of Information Security Management Standardization. *International Journal of Network Security, 18*(3), 565-578.

Hussein, R., Shahriza Abdul Karim, N., & Hasan Selamat, M. (2007). The impact of technological factors on information systems success in the electronic-government context. *Business Process Management Journal, 13*(5), 613-627.

Hwang, M.-S., Li, C.-T., Shen, J.-J., & Chu, Y.-P. (2004). Challenges in e-government and security of information. *Information & Security: An International Journal, 15*(1), 9-20.

Ibrahim, M. K., & Hamid, M. A. J. (2013). Secure E-Government Framework: Design and Implementation. *International Journal of Computer Science Engineering & Technology, 3*(5), 186-193.

Ikeda, A. A. (2009). Reflections on qualitative research in business. *REGE. Revista de Gestão, 16*(3), 49.

ISACA. (2012). Information Systems Audit and Control Association. Retrieved from http://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf

Ismail, R. B. (2012). *ASSESSING INFORMATION SECURITY MANAGEMENT IN MALAYSIAN ACADEMIC LIBRARIES.* (DOCTOR OF PHILOSOPHY), UNIVERSITY OF MALAYA

KUALA LUMPUR.

Ismail, Z., Masrom, M., Sidek, Z., & Hamzah, D. (2010). Framework to Manage Information Security for Malaysian Academic Environment. *Information Assurance & Cybersecurity, 2010*, 16.

ISO. (2005). ISO/IEC 27001:2005, Information technology -- Security techniques -- Information security management systems -- Requirements. Retrieved from ISO website: http://www.iso.org/iso/catalogue_detail?csnumber=42103

ITGI. (2013). IT Governance Institute. . Retrieved from http://www.itgi.org

Jaafar, J. T., Hamza, N., & Hassan, B. E. M. (2014). Security Model in E-government with Biometric based on PKI. *International Journal of Computer Applications, 93*(6).

Jankowicz, A. (2013). *Business Research Projects*: Springer.

Johnson, B., & Christensen, L. (2013). *Educational research: Quantitative, qualitative, and mixed approaches 5th Edition*: Sage.

Kankanhalli, A., Teo, H.-H., Tan, B. C., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International journal of information management, 23*(2), 139-154.

Kaptein, M. C., Nass, C., & Markopoulos, P. (2010). *Powerful and consistent analysis of likert-type ratingscales.* Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

Karunasena, K., & Deng, H. (2012). Critical factors for evaluating the public value of e-government in Sri Lanka. *Government Information Quarterly, 29*(1), 76-84.

Kasinath, H. (2013). Understanding and using qualitative methods in performance measurement. *MIER Journal of Educational Studies, Trends and Practices, 3*(1).

Katzan, H. (2012). Cybersecurity Service Model. *Journal of Service Science (Online), 5*(2), 71.

Kaur, J., Bahri, A. H. S., & Malaysia, M. (2014). IMPLEMENTATION OF INFORMATION TECHNOLOGY GOVERNANCE IN THE MALAYSIAN PUBLIC SECTOR PRACTICE.

Kaur, J., Mohamed, N., & Ahlan, A. R. (2012). *Modeling the impact of information technology governance effectiveness using partial least square.* Paper presented at the Statistics in Science, Business, and Engineering (ICSSBE), 2012 International Conference on.

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly executive, 9*(3), 2012-2052.

Kazemi, M., Khajouei, H., & Nasrabadi, H. (2012). Evaluation of information security management system success factors: Case study of Municipal organization. *African Journal of Business Management, 6*(14), 4982-4989.

Kessler, K., Hettich, N., Parsons, C., Richardson, C., & Triana, A. (2011). A Framework for Assessing Privacy Readiness of e-Government. . Retrieved from http://www.sed.manchester.ac.uk/idpm/research/publications/wp/igovernment/documents/iGovWkPpr21.pdf

Khine, M. S. (2013). *Application of structural equation modeling in educational research and practice*: Springer.

Kim, S.-S., & Jeoung, K.-H. (2015). Effects of Security Policies, Security Awareness of Hospital Employee to Patients' Personal Information Protection. *Indian Journal of Science and Technology, 8*(21).

Kline, R. B. (2015). *Principles and practice of structural equation modeling*: Guilford publications.

Knapp, K. J. (2005). *A Model of Managerial Effectiveness in Information Security: From grounded theory to empirical test*. Retrieved from

Knapp, K. J., & Ferrante, C. J. (2014). Information Security Program Effectiveness in Organizations: The Moderating Role of Task Interdependence. *Journal of Organizational and End User Computing (JOEUC), 26*(1), 27-46.

Knapp, K. J., Marshall, T. E., Rainer Jr, R. K., & Ford, F. N. (2007). Information security effectiveness: conceptualization and validation of a theory. *International Journal of Information Security and Privacy (IJISP), 1*(2), 37-60.

Knapp, K. J., Morris, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security, 28*(7), 493-508.

Kocak, C., Egrioglu, E., Yolcu, U., & Aladag, C. H. (2014). Computing Cronbach Alpha Reliability Coefficient for Fuzzy Survey Data. *American Journal of Intelligent Systems, 4*(5), 204-213.

Koskosas, I., Kakoulidis, K., & Siomos, C. (2011). Information Security: Corporate Culture and Organizational Commitment. *Int. J. Humanit. Soc. Sci, 1*(3), 192-198.

Koufteros, X. A. (1999). Testing a model of pull production: a paradigm for manufacturing research using structural equation modeling. *Journal of Operations Management, 17*(4), 467-488.

Kowalski, S. (1994). *IT Insecurity: A Multi-disciplinary Inquiry*. Retrieved from Stockholm:

Kowalski, S. (1994). *IT Insecurity: A Multi-disciplinary Inquiry*: Univ.

Kraemer, S., & Carayon, P. (2005). *Computer and information security culture: findings from two studies.* Paper presented at the Proceedings of the Human Factors and Ergonomics Society Annual Meeting.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *computers & security, 28*(7), 509-520.

Krebs, B. (2014). Home depot: Hackers stole 53m email addresses. *Krebs on Security*.

Kumar, A. (2015). Review of the Steps for Development of Quantitative Research Tools. Adv Practice Nurs 1: 103. doi: 10.4172. *APN, 1000103*, 2.

Kunnathur, A. S. (2015). Information security in supply chains: a management control perspective. *Information & Computer Security, 23*(5), 476-496.

Laursen, B., Little, T. D., & Card, N. A. (2012). *Handbook of developmental research methods*: Guilford Press.

Layne, K., & Lee, J. (2001). Developing fully functional E-government: A four stage model. *Government information quarterly, 18*(2), 122-136.

Lean, O. K., Zailani, S., Ramayah, T., & Fernando, Y. (2009). Factors influencing intention to use e-government services among citizens in Malaysia. *International Journal of Information Management, 29*(6), 458-475.

Leary, M. R., Kelly, K. M., Cottrell, C. A., & Schreindorfer, L. S. (2013). Construct validity of the need to belong scale: Mapping the nomological network. *Journal of Personality Assessment, 95*(6), 610-624.

Lee, S. M., Lee, S.-G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management, 41*(6), 707-718.

Leow, R. P. (2015). *Explicit learning in the L2 Classroom: A student-centered approach*: Routledge.

Lim, J. S., Ahmad, A., Chang, S., & Maynard, S. B. (2010). *Embedding Information Security Culture Emerging Concerns and Challenges*. Paper presented at the PACIS.

Loch, K. D., & Carr, H. H. (1991). *Threats to information system security: an organizational perspective*. Paper presented at the System Sciences, 1991. Proceedings of the Twenty-Fourth Annual Hawaii International Conference on.

Loser, K.-U., Nolte, A., Herrmann, T., & Neues, H. T. (2011). *Information security management systems and socio-technical walkthroughs*. Paper presented at the Socio-Technical Aspects in Security and Trust (STAST), 2011 1st Workshop on.

Loukis, E., & Spinellis, D. (2001). Information systems security in the Greek public sector. *Information management & computer security, 9*(1), 21-31.

Lu, C.-S., Lai, K.-h., & Cheng, T. E. (2007). Application of structural equation modeling to evaluate the intention of shippers to use Internet services in liner shipping. *European Journal of Operational Research, 180*(2), 845-867.

Ma, Q., Johnston, A. C., & Pearson, J. M. (2008). Information security management objectives and practices: a parsimonious framework. *Information Management & Computer Security, 16*(3), 251-270.

Malhotra, N. K. (2010). *Marketing research: An applied orientation* (Vol. 834).

Malhotra, N. K., Hall, J., Shaw, M., & Oppenheim, P. (2004). *Essentials of marketing research: an applied orientation*: Pearson Education Australia.

Markaki, O. I., Charilas, D. E., & Askounis, D. (2010). Evaluation of the Impact and Adoption of E-government Services in the Balkans *Comparative E-Government* (pp. 91-114): Springer.

Markus, K. A. (2012). Principles and Practice of Structural Equation Modeling by Rex B. Kline. *Structural Equation Modeling: A Multidisciplinary Journal, 19*(3), 509-512.

Mathews, A. W., & Yadron, D. (2015). Health insurer anthem hit by hackers. *Cit, 2*, 5-15.

Maumbe, B. M. (2009). *E-Agriculture and E-Government for Global Policy Development: Implications and Future Directions: Implications and Future Directions*: IGI Global.

May, L., & Lane, T. (2006). A Model for Improving e-Security in Australian Universities. *JTAER, 1*(2), 90-96.

Mears, L., & von Solms, R. (2004). *Corporate information security governance: a holistic approach.* Paper presented at the ISSA 2004 enabling tomorrow Conference, eds. HS Venter, JHP Eloff, L. Labuschagne & MM Eloff, Information Security For South Africa, Johannesburg.

Mesquida, A. L., Mas, A., Amengual, E., & Calvo-Manzano, J. A. (2012). IT Service Management Process Improvement based on ISO/IEC 15504: A systematic review. *Information and Software Technology, 54*(3), 239-247.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia-Social and Behavioral Sciences, 147*, 424-428.

Michael, Whitman, & Mattord, H. J. (2007). *Principles of Information Security,* (3rd Edition ed.).

Mindrila, D. (2010). Maximum likelihood (ML) and diagonally weighted least squares (DWLS) estimation procedures: A comparison of estimation bias with ordinal and multivariate non-normal data. *International Journal of Digital Society, 1*(1), 60-66.

Mishra, S., & Chasalow, L. (2014). INFORMATION SECURITY EFFECTIVENESS: A RESEARCH FRAMEWORK.

Mohd Alwi, N. H., & Fan, I.-S. (2010). E-learning and information security management. *International Journal of Digital Society (IJDS), 1*(2), 148-156.

Moon, M. J. (2002). The Evolution of E-Government among Municipalities: Rhetoric or Reality? *Public administration review, 62*(4), 424-433.

Mora, M. (2012). *Research Methodologies, Innovations and Philosophies in Software Systems Engineering and Information Systems*: IGI Global.

Moutinho, L., & Hutcheson, G. D. (2011). *The SAGE dictionary of quantitative management research*: Sage.

Mvungi, N. H., & Makoko, M. (2012). *Information System Security Effectiveness Attributes: A Tanzanian Company Case Study*. Paper presented at the Proceedings of World Academy of Science, Engineering and Technology.

Mwakalinga, J. (2011). A Framework for Adaptive Information Security Systems: A Holistic Investigation.

Myers, M. D. (2013). *Qualitative research in business and management*: Sage.

Naik, K. S., Ramachandra, G., & Reddy, M. B. (2014). An Extended Security Framework for E-Government. *International Journal of Advanced Research in Computer Science, 5*(1).

Narain Singh, A., Gupta, M., & Ojha, A. (2014). Identifying factors of "organizational information security management". *Journal of Enterprise Information Management, 27*(5), 644-667.

Neuman, W. L. (2009). *Social Research Methods: Qualitative and Quantitative Approaches (7th Edition)* Pearson.

Neuman, W. L., & Robson, K. (2012). Basics of social research: Qualitative and quantitative approaches.

Ngo, L., Zhou, W., & Warren, M. (2005). *Understanding Transition towards Information Security Culture Change*. Paper presented at the AISM.

O'Rourke, N., Psych, R., & Hatcher, L. (2013). *A step-by-step approach to using SAS for factor analysis and structural equation modeling*: Sas Institute.

Olusegun, O. J., & Ithnin, N. B. (2013). Enhancing the Conventional Information Security Management Maturity Model (ISM3) in Resolving Human Factors in Organization Information Sharing. *arXiv preprint arXiv:1309.0189*.

Oseni, K., Dingley, K., & Hart, P. (2015). E-service security: taking proactive measures to guide against theft, case study of developing countries. *International Journal for e-Learning Security, 5*(2), 454-461.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' behavior towards IS security policy compliance.* Paper presented at the System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on.

Pallant, J. (2007). SPSS survival manual: A step-by-step guide to data analysis using SPSS version 15. *Maidenhead, Berkshire, England: McGraw-Hill Education.*

Pallant, J. (2013). *SPSS survival manual*: McGraw-Hill Education (UK).

Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). *Human factors and information security: individual, culture and security environment.* Retrieved from

Paulsen, C., & Coulson, T. (2014). Beyond Awareness: Using Business Intelligence to Create a Culture of Information Security. *Communications of the IIMA, 11*(3), 4.

Pett, M. A., Lackey, N. R., & Sullivan, J. J. (2003). *Making sense of factor analysis: The use of factor analysis for instrument development in health care research*: Sage.

Pulkkinen, M., Naumenko, A., & Luostarinen, K. (2007). Managing information security in a business network of machinery maintenance services business–enterprise architecture as a coordination tool. *Journal of Systems and Software, 80*(10), 1607-1620.

Radack, S. (2008). Using Performance Measurements to Evaluate and Strengthen Information System Security.

Ramachandran, S., Rao, S. V., & Goles, T. (2008). *Information security cultures of four professions: a comparative study.* Paper presented at the Hawaii International Conference on System Sciences, Proceedings of the 41st Annual.

Ramachandran, S., Rao, V. S. C., Goles, T., & Dhillon, G. (2013). Variations in Information Security Cultures across Professions: A Qualitative Study. *Communications of the Association for Information Systems, 33*(1), 11.

Ramli, R. M. (2012). Malaysian e-government: issues and challenges in public administration. *International Proceedings of Economic Development and Research, 48*(2), 19-23.

Ritchie, J., Lewis, J., Nicholls, C. M., & Ormston, R. (2013). *Qualitative research practice: A guide for social science students and researchers*: Sage.

Robbins, S. P., & Judge, T. A. (2012). *Organizational Behavior 15th Edition*: prentice Hall.

Rorissa, A., & Demissie, D. (2010). An analysis of African e-Government service websites. *Government Information Quarterly, 27*(2), 161-169.

Rose, W. R., & Grant, G. G. (2010). Critical issues pertaining to the planning and implementation of E-Government initiatives. *Government Information Quarterly, 27*(1), 26-33.

Rotvold, G. (2008). How to create a security culture in your organization: a recent study reveals the importance of assessment, incident response procedures, and social engineering testing in improving security awareness programs. *Information Management Journal, 42*(6), 32-38.

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security, 26*(1), 56-62.

Ruighaver, A. B., Maynard, S. B., & Warren, M. (2010). Ethical decision making: Improving the quality of acceptable use policies. *Computers & security, 29*(7), 731-736.

S.Corporation. (2014). Internet security threat report 2014. Retrieved from Symantec Corporation website: http://www.symantec.com/content/en/us/enterprise/other_resources/bistr_main_report_v19_21291018.en-us.pdf

Sahi, G., & Madan, S. (2012). Information Security Threats in ERP Enabled E-Governance. *Strategic Enterprise Resource Planning Models for E-Government: Applications and Methodologies*, 158.

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal, 39*(4), 60-66.

Salih, E. H., Diwan, S. A., & Fattah, A. J. (2013). Multi-Agent Based Security Framework for E-Government in Recently technology Developed Countries. *Computer Engineering and Intelligent Systems, 4*(11), 34-42.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students*: Pearson Education.

Saunders, M. N. (2011). *Research methods for business students, 5/e*: Pearson Education India.

Savalei, V., & Bentler, P. M. (2010). Structural equation modeling. *Corsini encyclopedia of psychology*.

Schein, E. (2009). The Corporate Culture Survival Guide, San Francisco, J: Wiley and Sons.

Schlienger, T., & Teufel, S. (2002). *Information Security Culture: The Socio-Cultural Dimension in Information Security Management.* Paper presented at the Proceedings of the IFIP TC11 17th International Conference on Information Security: Visions and Perspectives.

Schlienger, T., & Teufel, S. (2003). Information security culture-from analysis to change. *South African Computer Journal*(31), p. 46-52.

Schlienger, T., & Teufel, S. (2005). Tool supported management of information security culture *Security and Privacy in the Age of Ubiquitous Computing* (pp. 65-77): Springer.

Schumacker, R. E., & Lomax, R. G. (2016). *A Beginner's Guide to Structural Equation Modeling: Fourth Edition*: Routledge.

Schweizer, K. (2014). On the ways of investigating the discriminant validity of a scale in giving special emphasis to estimation problems when investigating multitrait-multimethod matrices.

Seifert, J. W., & Petersen, R. E. (2002). The promise of all things E? Expectations and challenges of emergent electronic government. *Perspectives on Global Development and Technology, 1*(2), 193-212.

Sekaran, U. (2003). *Research methods for business: A skill building approach*: John Wiley & Sons.

Sekaran, U., & Bougie, R. (2010). *Research Methods for Business: A Skill Building Approach*: John Wiley & Sons.

Seltman, H. J. (2012). Experimental design and analysis. *Online at: http://www. stat. cmu. edu/, hseltman/309/Book/Book. pdf.*

Setiadi, F., Sucahyo, Y. G., & Hasibuan, Z. A. (2013). *Balanced E-Government security framework: An integrated approach to protect information and application.* Paper presented at the Technology, Informatics, Management, Engineering, and Environment (TIME-E), 2013 International Conference on.

Shaaban, H. K. (2014). Enhancing the governance of information security in developing countries: the case of Zanzibar.

Shah, R., & Goldstein, S. M. (2006). Use of structural equation modeling in operations management research: Looking back and forward. *Journal of Operations Management, 24*(2), 148-169.

Shahri, A. B., Ismail, Z., & Rahim, N. Z. A. (2013). Security Culture and Security Awareness as the Basic Factors for Security Effectiveness in Health Information Systems. *Jurnal Teknologi, 64*(2).

Shayan, A., Abdi, B., & Qeisari, M. (2010). Identification of the required security practices during e-government maturity *Global Security, Safety, and Sustainability* (pp. 250-262): Springer.

Siau, K., & Long, Y. (2005). Synthesizing e-government stage models–a meta-synthesis based on meta-ethnography approach. *Industrial Management & Data Systems, 105*(4), 443-458.

Singh, S., & Karaulia, D. S. (2011). *E-Governance: Information Security Issues.* Paper presented at the International Conference on Computer Science and Information Technology (ICCSIT'2011) Pattaya.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: an empirical investigation. *Computer, 43*(2), 64-71.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly, 34*(3), 487.

Siponen, M., Willison, R., & Baskerville, R. (2008). Power and practice in information systems security research. *ICIS 2008 Proceedings*, 26.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM Sigmis Database, 38*(1), 60-80.

Stevens, J. P. (2012). *Applied multivariate statistics for the social sciences*: Routledge.

Strang, K. D. (2015). *The Palgrave Handbook of Research Design in Business and Management*: Palgrave Macmillan.

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *The Communications of the Association for Information Systems, 13*(1), 63.

Straub, D., Limayem, M., & Karahanna-Evaristo, E. (1995). Measuring system usage: Implications for IS theory testing. *Management science, 41*(8), 1328-1342.

Straub Jr, D. W. (1990). Effective IS Security. *Information Systems Research, 1*(3), 255-276.

Suduc, A.-M., Bizoi, M., & Filip, F. G. (2010). Audit for Information Systems Security. *Informatica Economica, 14*(1), 43-48.

Suhr, D., & Shay, M. (2009). *Guidelines for reliability, confirmatory and exploratory factor analysis.* Paper presented at the Proc. 2009 Western Users of SAS Conf. San Jose, CA.

Symantec, T. (2009). Symantec internet security threat report trends for 2008.

Tabachnick, B., & Fidell, L. (2013). Using multivariate statistics (6th international edition (cover). ed.): Boston,[Mass.].

Taiwo, A. A., Mahmood, A. K., & Downe, A. G. (2012). *User acceptance of eGovernment: Integrating risk and trust dimensions with UTAUT model.* Paper presented at the Computer & Information Science (ICCIS), 2012 International Conference on.

Tambouris, E. (2001). *An integrated platform for realising online one-stop government: the eGOV project.* Paper presented at the Database and Expert Systems Applications, 2001. Proceedings. 12th International Workshop on.

Tarimo, C. N. (2006). *ICT security readiness checklist for developing countries: A social-technical approach.* Stockholm.

Tarimo, C. N., Bakari, J. K., Yngström, L., & Kowalski, S. (2006). *A Social-Technical View of ICT Security Issues, Trends, and Challenges: Towards a Culture of ICT Security-The Case of Tanzania.* Paper presented at the ISSA.

Tashakkori, A., & Teddlie, C. (1998). *Mixed methodology: Combining qualitative and quantitative approaches* (Vol. 46): Sage.

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International journal of medical education, 2*, 53.

Tojib, D. R., & Sugianto, L.-F. (2011). Construct validity assessment in IS research: methods and case example of user satisfaction scale. *Journal of Organizational and End User Computing (JOEUC), 23*(1), 38-63.

U.S E-Government Act of (2002). Retrieved from http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

Upadhyaya, P., Nguyen, T. A., Pokharel, M., & Shakya, S. (2013). Modeling and Analysis of High availability Security Architecture for Whole of Government Systems. *American Journal of Computer Science and Engineering Survey (AJCSES), 1*(1), 58-69.

Vaishnavi, V. K., & Kuechler Jr, W. (2007). *Design science research methods and patterns: innovating information and communication technology*: CRC Press.

Van Niekerk, J., & von Solms, R. (2006). *Understanding Information Security Culture: A Conceptual Framework.* Paper presented at the ISSA.

Van Niekerk, J., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security, 29*(4), 476-486.

Veiga, A. D., & Eloff, J. H. (2007). An information security governance framework. *Information Systems Management, 24*(4), 361-372.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security, 38*, 97-102.

Wang, J.-f. (2009). *E-government security management: key factors and countermeasure.* Paper presented at the Proceedings of the 2009 Fifth International Conference on Information Assurance and Security-Volume 02.

Wangwe, C. K. (2012). *Towards an information security framework for government to government transactions: a perspective from East Africa.* University of South Africa.

Waziri, M. D., & Yonah, Z. O. (2014). A Secure Maturity Model for Protecting e-Government Services: A Case of Tanzania. *Advances in Computer Science: an International Journal, 3*(5), 98-106.

Weerakkody, V., El-Haddadeh, R., Sabol, T., Ghoneim, A., & Dzupka, P. (2012). E-government implementation strategies in developed and transition economies: A comparative study. *International Journal of Information Management, 32*(1), 66-74.

West, D. M. (2004). E-Government and the Transformation of Service Delivery and Citizen Attitudes. *Public administration review, 64*(1), 15-27.

Wipawayangkool, K. (2009). Security awareness and security training: An attitudinal perspective. *SWDSI 2009*, 266-273.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816.

Yeh, Q.-J., & Chang, A. J.-T. (2007). Threats and countermeasures for information system security: A cross-industry study. *Information & Management, 44*(5), 480-491.

Yonazi, J. J. (2010). *Enhancing adoption of e-government initiatives in Tanzania.* University of Groningen.

Yong, A. G., & Pearce, S. (2013). A beginner's guide to factor analysis: Focusing on exploratory factor analysis. *Tutorials in Quantitative Methods for Psychology, 9*(2), 79-94.

Zhao, D. (2011). *On Several Major Issues of the Construction of Chinese E-government Information Security System.* Paper presented at the Business Computing and Global Informatization (BCGIN), 2011 International Conference on.

Zikmund, W., Babin, B., Carr, J., & Griffin, M. (2012). *Business research methods*: Cengage Learning.

Appendix A: CONSENT FORM

UNIVERSITI SAINS ISLAM MALAYSIA
جامعة العلوم الإسلامية الماليزية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA
FACULTY OF SCIENCE AND TECHNOLOGY
Fakulti Sains dan Teknologi
كلية العلوم والتكنولوجيا

Consent Form

Dear Prospective Participant,

My name is Rabia Ihmouda; I am a Doctoral candidate of Information Security Assurance program, Faculty of Science and Technology, Universiti Sains Islam Malaysia.

My research area is developing a socio-technical security framework that would facilitate government organizations to effectively offer appropriate secure e-government services.

This questionnaire aims to examine the influence of socio-technical factors related to the information security in organizations, to develop an **information security culture framework which will improve e-government security effectiveness in developing countries**

This research is planned to be conducted in Malaysia, your organizations have been selected as a case study.

Procedure & Duration: Your valued participation involves completing the enclosed questionnaire, which includes background questions, and statements about your perception of information security practices. This study will take approximately 20-25 minutes.

Voluntary Nature: Participation is voluntary and responses will be kept confidential. You have the option to not respond to any survey questions that you choose. Also, please note that the information presented in this questionnaire will only be used for the intended purposes and will be treated as confidential.

Risks & Benefits: You will not be asked for any personal information that could identify you. This ensures your anonymity, confidentially and privacy, All data will be used only for research purposes. The data collected will provide useful information for improving the security effectiveness regarding to Malaysian e-government.

Thank you in advance for your valuable time and consideration.

Contact information:

Dr. Najwa Hayaati Mohd Alwi
Research Supervisor
Faculty of Science and Technology
Universiti Sains Islam Malaysia
najwa@usim.edu.my

Rabia Ihmouda Hassan
PhD Candidate
Faculty of Science and Technology
Universiti Sains Islam Malaysia
rbhamouda@yahoo.com

Appendix B: QUESTIONNAIRE

UNIVERSITI SAINS ISLAM MALAYSIA
جامعة العلوم الإسلامية الماليزية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA
FACULTY OF SCIENCE AND TECHNOLOGY
Fakulti Sains dan Teknologi
كلية العلوم والتكنولوجيا

QUESTIONNAIRE: Information Security Practices

Section I: Background

Please take a few minutes to answer carefully the questions on the following pages by mark (√) in the right place or filling in the blanks.

- **Gender:**

  ○ Male ○ Female

- **Qualification**

  ○ Bachelor ○ Master ○ PhD

- **Years of Experience**

○ Less than 5 ○ From 5 – less than 10 ○ From10–less than 15 ○ Above 15 years

- **Job task**

○ Department/Operational Manager ○ Chief Information Officer ○ IT Manager

○ Security Manager ○ Security Officer ○ IT Staff

○ Security Staff ○ Operation Staff (e.g., Administrator, Clerical) ○ Technical Staff

Section II: Information Security Practices Statements

Number 1-5 represents your response to the statement. Please read each statement carefully and mark (√) on a box that you think represents most appropriate choice for your response

Strongly disagree	Disagree	Undecided	Agree	Strongly agree
1	2	3	4	5

Ethical/Cultural - 2006)	Ethical conduct (EC) In my organization…(Chaula,	1	2	3	4	5
EC1	In the course of my professional activities, I shall conduct myself in accordance with the highest standards of moral, ethical and legal behavior.	○	○	○	○	○
ET2	I always Identify, define and address ethical, cultural, and legal issues related to work projects.	○	○	○	○	○
ET3	I will appropriately report any use of property of a client or employer in ways which are unauthorized, and without the clients or employer's knowledge and consent.	○	○	○	○	○
Legal/Contractual -	Legal (L) in my organization…	1	2	3	4	5
L1	The legislations for e-government are in place. (Altameem, 2007)	○	○	○	○	○
L2	Policy is updated when legal & regulatory changes require it. (Knapp et al.,	○	○	○	○	○

	2006)					
L3	Information security policies are written with the proper understanding of legal requirements. (Knapp et al., 2006)	○	○	○	○	○
L4	The policy covers the legal aspects of security (KPMG, 2012)	○	○	○	○	○
	Information Security Compliance (IC) in my organization…	1	2	3	4	5
IC1	I always adhere to the information security policy.(Chaula, 2006)	○	○	○	○	○
IC2	Information security measures comply with international standards(Chaula, 2006)	○	○	○	○	○
IC3	I comply with information security with international standards (Chaula, 2006)	○	○	○	○	○
Administrative/Managerial -	Top Management Support (TM) in my organization.	1	2	3	4	5
TM1	Top management takes security issues into account when planning corporate strategies. (Knapp et al., 2006)	○	○	○	○	○
TM2	Senior leadership's words and actions demonstrate that security is a priority.(Alnatheer, 2012)	○	○	○	○	○
TM3	Visible support for security goals by senior management is obvious.(Knapp et al., 2006)	○	○	○	○	○
TM4	Senior management gives strong and consistent support to the security program. (Knapp et al., 2006)	○	○	○	○	○
Operational/Procedural-	Information security policy (IP) In my organization…	1	2	3	4	5
IP1	Policy clearly defines information security objectives.(Narain Singh et al., 2014)	○	○	○	○	○
IP2	The information security policy clearly defines roles and responsibilities of employees. (Narain Singh et al., 2014)	○	○	○	○	○
IP3	The information security policy is reviewed regularly (or when the environment changes). (Narain Singh et al., 2014)	○	○	○	○	○
	Information Security Training (T) in my organization…	1	2	3	4	5
T1	Users receive adequate security refresher training appropriate for their job function (Knapp et al., 2007)	○	○	○	○	○
T2	I am always educated or trained about new security policies (Knapp et al., 2007)	○	○	○	○	○
T3	Education and learning are encouraged and supported. . (Altameem, 2007)	○	○	○	○	○
	Information security awareness (AW) in my organization…	1	2	3	4	5

AW1	I am aware of any information security policy in my organizations (Alnatheer, 2012)	○	○	○	○	○
AW2	Information security awareness is communicated well. (Knapp et al., 2007)	○	○	○	○	○
AW3	The e-government awareness policies are regularly used. (Altameem, 2007)	○	○	○	○	○
AW4	An effective security awareness program exists. (Knapp et al., 2007)	○	○	○	○	○
Information system structure (IS) in my organization…		1	2	3	4	5
ISS1	IT infrastructure is ready for the e-government initiatives. (Alfawaz, 2011)	○	○	○	○	○
ISS2	IT infrastructures accommodate integration with e-government. (Altameem, 2007)	○	○	○	○	○
ISS3	The IT infrastructure is continuously improved.(Altameem, 2007)	○	○	○	○	○
Security culture (SC) in my organization…		1	2	3	4	5
SC1	A culture exists that promotes good security practices. (Knapp & Ferrante, 2014)	○	○	○	○	○
SC2	Security has traditionally been considered an important organizational value.(Knapp & Ferrante, 2014)	○	○	○	○	○
SC3	Practicing good security is the accepted way of doing business. (Knapp & Ferrante, 2014)	○	○	○	○	○
SC4	Information security is a key norm shared by organizational members.(Knapp & Ferrante, 2014)	○	○	○	○	○
Security effectiveness (EF) in my organization…		1	2	3	4	5
EF1	The information security program achieves most of its goals. (Knapp & Ferrante, 2014)	○	○	○	○	○
EF2	The information security program has kept risks to a minimum.(Knapp & Ferrante, 2014)	○	○	○	○	○
EF3	Current information security measures provide effective protection for electronic data. (Spicer, 2004)	○	○	○	○	○
EF4	Overall, the information security program is effective. (Knapp & Ferrante, 2014)	○	○	○	○	○

Appendix C: Expert Review Questionnaire

UNIVERSITI SAINS ISLAM MALAYSIA
جامعة العلوم الإسلامية الماليزية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA
FACULTY OF SCIENCE AND TECHNOLOGY
Fakulti Sains dan Teknologi
كلية العلوم والتكنولوجيا

Consent Form

Dear Prospective Participant,

My name is Rabia Ihmouda; I am a Doctoral candidate of Information Security Assurance program, Faculty of Science and Technology, Universiti Sains Islam Malaysia.

Information Security Management (ISM) as practiced as a top down approach in many organizations tends to detach system user's sense of responsibility in ensuring the security of e-government. Literature has pointed out that people's behavior should be addressed to manage information security threats.

This research proposes an information security culture framework that would facilitate government organizations to effectively offer appropriate secure e-government services in developing countries (Figure 1 in Attachment A). Adopting a socio-technical approach, this framework aims to improve the implementation and management of e-government information security by targeting different stakeholders with controls relevant to their behavior cultural view.

The experts are invited to review the framework designed and to answer the questions. (Attachment B)

Thank you in advance for your valuable time and consideration.

Contact information:

Dr. Najwa Hayaati Mohd Alwi
Research Supervisor
Faculty of Science and Technology
Universiti Sains Islam Malaysia
najwa@usim.edu.my

Rabia Ihmouda Hassan
PhD Candidate
Faculty of Science and Technology
Universiti Sains Islam Malaysia
rbhamouda@yahoo.com

Questions

1. The framework is clear and easily understandable

2. The framework adequately addresses: technical, socio-technical, practice, and theory related security issues

3. The framework is aligned with current security standards and best practices

4. The framework is dynamic enough to deal with possible future security risks and threats

5. What is your overall impression about the new framework?

6. Do you feel that the framework can be used as security architecture for developing countries e-government?

7. What are your general comments on the framework?

8. Any additional suggestions to the framework?