VOL. 10, NO 20, NOVEMBER, 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

SUCCESSFUL FACTORS ON E-GOVERNMENT SECURITY SOCIAL-TECHNICAL ASPECT

Rabia Ihmouda, Najwa Hayaati Mohd Alwi and Ismail Abdullah
Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM), Negeri Sembilan, Malaysia
E-Mail: rbhamouda@yahoo.com

ABSTRACT

This study explored and identified success social-technical factors related to the information security effectiveness in organizations. It explored these factors based on literature view, and documents, the study based on the Socio-Technical approach (STA) and the Security by Consensus (SBC) model. Quantitative analysis of the organizations' employees' experiences were analyzed and discussed to validate the questionnaire. The aim of this paper is to propose conceptual framework for understanding, clarification and investigation of the socio-technical factors involved in improving e-government security effectiveness in developing countries.

Keywords: E-government, information security, social-technical factors, security effectiveness.

INTRODUCTION

Electronic Government is at the forefront of current public sector reform policies across the rest of the world, where the use of computer-based information and communication technologies to deliver public services in the public sector is seen as a major leverage of public sector innovation. E-government is usually presented as using Information and Communication Technologies (ICTs) to provide easy access to government information, increase the quality of services, and reduce the cost of services.

Nowadays, organizations need to work with their business partners or clients through communication networks. Where there is data exchange en route, there will be security problems. The security is considered one of the most important factors for achieving an advanced stage of e-government. As the number of e-government services increases, a higher level of e-government security is required [1, 2].

LITERATURE REVIEW

Information security management

Information Security (IS) is effective implementation of policies to ensure the confidentiality, availability and integrity of information and assets is protected from theft, tampering, manipulation or corruption [3]. The three aspects of data security are [4]:

- **Confidentiality:** refers to protection of information from unauthorized disclosure e.g. to the press or to release through improper disposal techniques, or to those who are not entitled to have the same.
- **Integrity:** is about protecting information from unauthorized modification, and ensuring that information, such as a beneficiary list, can be relied upon and is accurate and complete.
- **Availability:** is to ensure that the information is available when it is required.

Information security management (ISM) is the means by which we ensure that we are taking account of these three factors. The purpose of ISM is to promote the confidence and the effectiveness of information services within an organization, or between an organization and its business partners [5].

Information Security Magazine (2002) conducted survey showed that the most information security problems were caused by the negligence of people, rather by attack events. Therefore, it is important to train and manage the problem-prone people [6]. The information security is not primarily a technical problem but a management or business issue [7-9].

However, a security system can be effective by the attitudes and behaviors of the people that interact with the system. This makes people an important part of the security system.

Socio-technical approach

The study was based on the Socio-Technical approach (STA) and the Security By Consensus (SBC) model [10]. Socio-technical systems theory has been used for decades as a framework to design and understand organizations.

- **Socio-Technical model (STM)**

Kowalski [10] developed Socio-technical security system for protecting information. The model is depicted in Figure-1. This has two sub-systems include Social (culture and structures) and Technical (methods and machines).

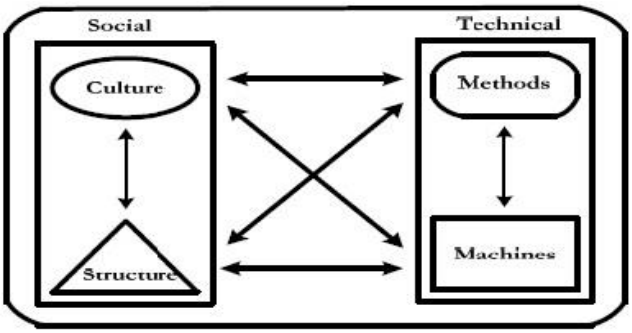

Figure-1. Socio-Technical model [10].

- **SBC model**

The Security by Consensus (SBC) model was applied to define the detailed parts of Socio-technical model (STM) subsystem controls, detailed in Figure-2.

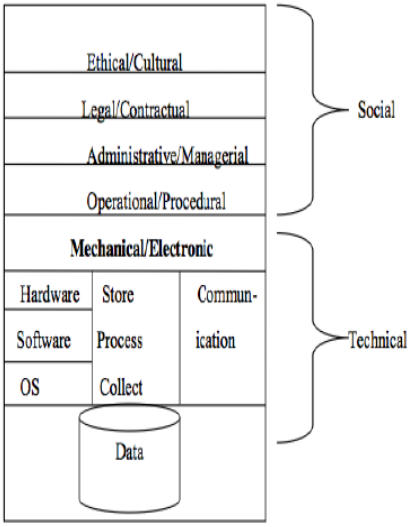

Figure-2. The basic SBC model [10].

A better model of security is the SBC model proposed by Kowalski [10] which gives a more useful description of security [11]. The model divides with two basic components of a social subsystem and a technical subsystem, which are further divided into subclasses social (Ethical-cultural, Legal-contractual, Administrative-managerial-Policy, and Operational-procedural) and Technical (Mechanical-electronic and Information-Data).

Information system security effectiveness

Measuring the effectiveness of security in information systems (IS) is an issue that has seriously been questioned among academics and practitioners. According to Straub [12] IS security effectiveness is the ability of IS security measure to protect against unauthorized or deliberate misuse of IS assets of people.

Although, the literature focusing on information security effectiveness in organization is sparse, Table1 provides some of the literature on information security effectiveness models and frameworks.

Table-1. Summary of current information security effectiveness models and frameworks.

Authors	Model	Finding
Straub Jr [12]	Provided one of the first models on IS security effectiveness.	He investigated whether a management decision in IS security result is more effective control of computer abuse.
Kankanhalli, Teo, Tan, and Wei [13]	Proposed a conceptual model of IS security effectiveness.	The model includes organizational factors such as Organizational size, Top management support, and Industry type. They found that greater deterrent efforts and preventive measures can increase IS security effectiveness.
D'Arcy and Hovav [14]	They extended deterrence theory model.	The result showed that the security awareness is the most countermeasures against human factor in threats to information security.
Da Veiga and Eloff, [15]	They present a framework to develop an information security culture in an organization.	The framework focused on employee behavior and has investigated security effectiveness in terms of security culture.
Herath and Rao [16]	They assessed the effectiveness of the security model consist of various motivating factors such as penalties, pressures and perceived contribution that encourages information security behaviors in organizations.	The study mentioned that creating a general culture that fosters security is a better strategy in information security
Brady [17]	Suggested a theoretical model for HIPAA security compliance in U.S.A academic medical centers.	The model showed that the management support, security awareness and security culture were important for security effectiveness.
Shahri, Ismail, and Rahim [18]	Proposed security effectiveness framework for health information systems.	The results of this study showed the importance of security culture and security awareness in establishing the security effectiveness for HIS

Literature review of different models and frameworks on IS security-related works have emphasize that through implementing all the required information security components, organizations must govern information security effectively [15-17, 19, 20]. Different information security components such as human factors, organizational factors, and technical factors can be used to compile a new comprehensive information security effectiveness framework.

RESEARCH METHODOLOGY

This study adopted mixed method to achieve the research aim; it was conducted in two stages:

The first stage: A systematic approach and extensive search on secondary data resources was executed in delimitating construct related to e-government security effectiveness and to develop survey questions. An exploration through on-line search was carried out among the various search engines.

The online databases that were given particular attention include: ACM digital library, EBSCO host, Elsevier Science Direct, Emerald Library, IEEE Electronic Library, IGI Global, Springer Link, and Taylor and Francis Group. The first findings of this study are identifying socio-technical factors that influence information security effectiveness in e-government context. Then, analysis and revision of literature show a clear need for socio-technical factors to be address for develop a security effectiveness framework. Therefore, the study proposes a framework based on mentioned factors to implement the security effectiveness in e-government.

The second stage is to validate the questionnaire, a survey distributed to twenty IT staffs practitioners from computer center of Universiti Sains Islam Malaysia (USIM).

SOCIO-TECHNICAL FACTORS

The objective of this study is to identify security socio-technical factors for information security effectiveness framework in the e-government domain. According to previous sections, by a review of current approaches towards e- government security and by putting together the literature on security effectiveness, socio-technical factors have identified in Table-2.

Table-2. Summary of Socio-technical factors influencing information security.

Constructs	Factors	Reference
Legal/Contractual	Legal and law	[15], [21, 22],[23], [24], [25]
	Compliance	[26], [27], [28], [29], [30]
Ethical/Cultural	Ethical Conduct	[15], [31], [29], [32]
	Organizational culture	[33], [34], [30]
Operational/Procedural	Information Security Policy	[15], [30], [26], [31], [29], [35]
	Security Awareness,	[28], [36], [35], [37], [38], [23]
	Information Security Training,	[26, 38], [31], [39], [29], [36]
	Incident management	[40], [30], [15], [19]
	Information Security Risk assessment,	[40], [15], [30], [15]
Administrative/Managerial	Top Management Support	[41], [36], [35], [13]
	Change Management	[40], [15], [30], [37], [19]
	Assist management	[40], [30], [15], [19]
Security culture		[31], [30, 38], [37], [17], [42], [43], [24]
IS structure		[33], [21], [23]
Security Effectiveness		[38], [44], [13], [44], [32], [17], [38]

INSTRUMENT VALIDATION

The questionnaire was developed based upon research literature, and distributed personally. IT is contained detailed brief and clear instructions [45]. Respondents were assured of privacy and confidentiality and they informed that from 20 to 25 minutes was the maximum time that needs to complete it.

Five-point Likert scales were applied to measure the perception of socio-technical factors influencing e-government security. In this study the numbers 1 to 5 were assigned to the categories of concepts (strongly disagree = 1, disagree = 2, undecided = 3, agree = 4 and strongly agree = 5), knowing that this surely does not represent the true distances between them but believing that it is close enough to derive meaningful results [45, 46]. The questionnaire was arranged as follows:

First Part - Background information. This is demographic questions in tick-list or short answer format.

Second Part- E-government related to critical security factors. Five-point Likert scales (1-5) to offer an agreement/disagreement level. This part was divided into five sections as follows:

- Ethical/Cultural Factors.
- Legal/Contractual Factors.
- Administrative/Managerial Factors.
- Operational/Procedural Factors.
- Mechanical/Electrical Factors.

The questionnaire was tested for content validity, construct validity, and reliability to ensure the questions were understood by the respondents and there were no problems with the wording of the instrument [45].

Content validity

The panel judgment method used for testing the draft questionnaire, through an 'expert-review' technique. This involved sending the draft questionnaire to a group of experts to judge whether each item measured the theoretical construct nominated. Four experts participated (academic staffs) in the review process. The experts were provided with a briefing sheet explaining the background and purpose of the study. The draft questionnaire was revised as per the experts' comments, resulting in the final survey questionnaire.

After revising the questionnaires, twenty participants conducted to evaluate the questionnaire for clarity, bias, ambiguous questions and relevance to the Malaysian environment, the tested sample size is small, varying from 15 to 30 responders for the initial test [47-49]. Twenty IT staff practitioners from computer center of Universiti Sains Islam Malaysia (USIM).

DATA ANALYSIS

Quantitative data were analyzed by first determining the number of valid and invalid responses, and then by developing a descriptive analysis of the data obtained revealing demographics of respondents, and other descriptive data about the research variables such as, means, standard deviations, etc. [50]. The researcher selected SPSS 20 program for serving this purpose.

Reliability

The reliability analysis was conducted to ensure the internal validity and consistency of the items used for each variables. Hair *et al.* (1998) [51] recommended that Cronbach alpha values greater than 0.6 were acceptable. Table-3 shows the Cronbach's alpha values greater than 0.7, which is considered very good [52], that mean the questionnaire is a reliable measurement instrument.

Table-3. Cronbach's Alpha for each field of the instrument.

No.	Paragraph	Number of Items	Cronbach's Alpha
1	Ethical Conduct (EC)	6	0.803
2	Organizational Culture (OC)	6	0.864
3	Legal and law (L)	8	0.860
4	Compliance (IC)	5	0.834
5	Top Management Support (TM)	8	0.920
6	Change Management (CM)	7	0.919
7	Incident management (IC)	7	0.883
8	Assist management (AM)	6	0.891
9	Information Security Policy (IP)	5	0.815
10	Information Security Training (T)	7	0.780
11	Security Awareness (AW)	7	0.848
12	Information Security Risk Assessment (RA)	5	0.934
13	IS Structure (IS)	5	0.894
14	Security Culture (SC)	5	0.776
15	Security Effectiveness (EF)	6	0.863
16	All paragraphs of the questionnaire	93	

Construct validity

Construct validity is established by determining whether the scores from an instrument are significant and can be used to understand a sample from a population [50]. Construct validity must meet the two following conditions: convergent and discriminant validity [53].

- **convergent validity** was assessed by factor loading, [54] and Average Variance Extracted (AVE) [55]. All factors loading should be significant and higher than .5 to showing good convergent validity [56]. In addition, if AVE more than 0.5 is acceptable [54]. (AVE) was calculated based on formula given by [55] .

$$AVE = \frac{\sum_{i=1}^{n} \lambda_i^2}{n}$$

AVE =Average variance extract
n = the number of items
λ= the standardized factor loading

Table-4. Factor loading for each for each Item of the instrument.

Construct	Item	Factor loading	AVE
Ethical Conduct	EC1	0.725	0.554
	EC2	0.782	
	EC3	0.627	
	EC4	0.800	
	EC5	0.884	
	EC6	0.611	
Organizational culture	OC1	0.807	0.747
	OC2	0.854	
	OC3	0.934	
	OC4	0.855	
	OC5	0.901	
	OC6	0.831	
Legal and law	L1	0.850	0.694
	L2	0.887	

	L3	0.860	
	L4	0.658	
	L5	0.768	
	L6	0.859	
	L7	0.894	
	L8	0.866	
Compliance	IC1	0.791	0.816
	IC2	0.945	
	IC3	0.878	
	IC4	0.986	
	IC5	0.907	
Top Management Support	TM1	0.878	0.699
	TM2	0.796	
	TM3	0.877	
	TM4	0.916	
	TM5	0.842	
	TM6	0.566	
	TM7	0.882	
	TM8	0.883	
Change Management	CM1	0.940	0.857
	CM2	0.897	
	CM3	0.899	
	CM4	0.978	
	CM5	0.955	
	CM6	0.895	
	CM7	0.916	
Incident management	IM1	0.886	0.679
	IM2	0.972	
	IM3	0.708	
	IM4	0.924	
	IM5	0.894	
	IM6	0.538	
	IM7	0.762	
Assist management	AM1	0.833	0.825
	AM2	0.893	
	AM3	0.967	
	AM4	0.833	
	AM5	0.960	
	AM6	0.953	
Information Security Policy	IP1	0.807	0.679
	IP2	0.823	
	IP3	0.681	
	IP4	0.929	
	IP5	0.862	
Information Security Training,	T1	0.741	0.652
	T2	0.787	
	T3	0.861	
	T4	0.603	
	T5	0.835	
	T6	0.894	
	T7	0.892	
Security Awareness,	AW1	0.627	0.589
	AW2	0.866	
	AW3	0.682	
	AW4	0.758	
	AW5	0.781	
	AW6	0.873	
	AW7	0.757	
Information Security Risk assessment,	RA1	0.741	0.632
	RA2	0.789	
	RA3	0.904	
	RA4	0.728	
	RA5	0.801	
IS structure	IS1	0.629	0.534
	IS2	0.780	
	IS3	0.936	
	IS4	0.642	
	IS5	0.617	
Security Culture	SC1	0.876	0.659
	SC2	0.666	
	SC3	0.833	
	SC4	0.908	
	SC5	0.753	
Security Effectiveness	EF1	0.909	0.681
	EF2	0.912	
	EF3	0.755	
	EF4	0.895	
	EF5	0.705	
	EF6	0.749	

As showing in Table-4 the factor loading of all items are greater than 0.5 which consider as acceptable level, and the AVE for all factor are in the acceptable level, the AVE ranges were between of 0.738 to 0.985.

- **Discriminant validity** refers to the extent to which a construct is truly distinct from other constructs [57]. Therefore, discriminant validity measurement should be uncorrelated with measures of unrelated constructs [58]. Discriminant validity can be measured using Fornell and Larcker criteria [55], where the level of square root of AVE should be greater than the correlations involving the constructs.

Table-5. Discriminant validity.

	EC	OC	L	IC	TM	CM	IM	AM	IP	T	AW	RA	IS	SC	EF
EC	0.744*														
OC	0.626	0.864*													
L	0751	0.653	0.833*												
IC	0.744	.0.747	.0.827	0.903*											
TM	0586	.0.675	.0.613	0.680	0.836*										
CM	0.828	0.804	0.818	.0.716	0.705	0.926*									
IM	.0.534	0.782	0.496	0.715	0.814	0.624	0.824*								
AM	0.637	0.814	0.483	0.624	0.561	0.574	0.727	0.908*							
IP	0.600	0.757	0.414	0.618	0.793	0.653	0.809	0.745	0.824*						
T	.089	0.436	0.456	0.379	0.398	0.395	0.545	0.311	0.328	0.807*					
AW	0.359	0.687	0.566	0.638	0.737	0.532	0.694	0.557	0.599	0.403	0.767*				
RA	0.703	0.585	0.529	0.587	0.688	0.684	0.806	0.610	0.802	0.468	0.377	0.825*			
IS	0.409	0.647	0.396	0.488	0.535	0.531	0.814	0.716	0.724	0.684	0.566	0.767	0.831*		
SC	0.726	0.702	0.611	0. 623	0.844	0.771	0.788	0.707	0.888	0.304	0.591	.843	0.666	0.891*	
EF	0.478	0.477	0.430	0.506	0.495	0.405	0.674	0.598	0.638	0.516	0.385	0.791	0.678	0.571	0.825*

As showing in Table-5 the results of testing convergent validity revealed good construct validity.

CONCEPTUAL FRAMEWORK DEVELOPMENT

A conceptual security effectiveness framework for e-government information systems was constructed from the Socio-Technical approach (STA), the Security By Consensus (SBC) model, and adapting earlier work [12, 13] to address concerns about security effectiveness. Figure-3 describes that a relationship may be between socio-technical factors with security effectiveness in e-government.

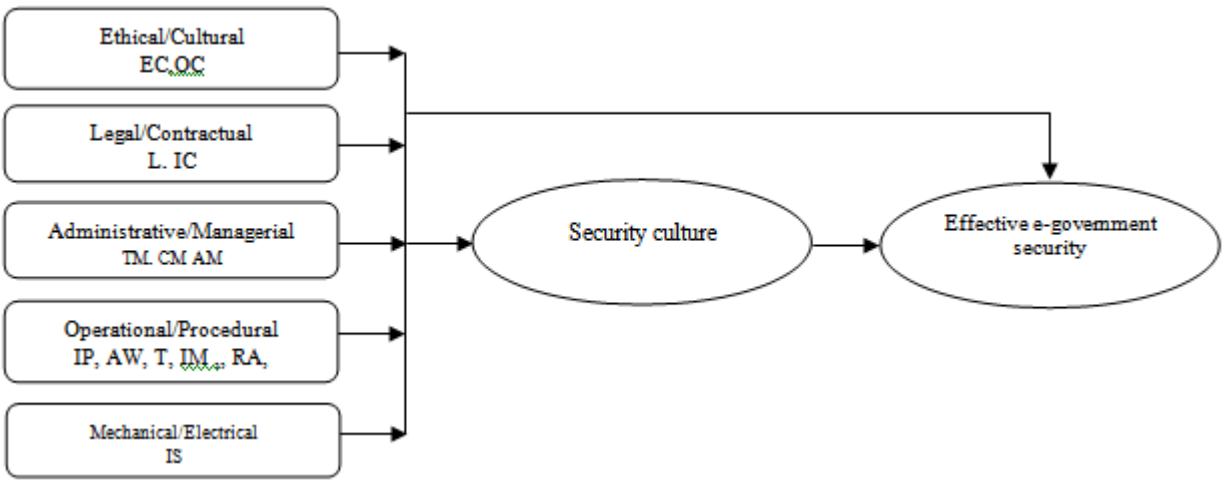

Figure-3. The conceptual framework of socio-technical factors influence the information security effectiveness.

CONCLUSIONS

This study had succeeded in identifying the socio-technical factors that influence information security. Based on secondary data, Legal/ Contractual, Ethical/Cultural, Operational/Procedural, Administrative/ Managerial, Mechanical/ Electrical, play a role in influencing information security effectiveness. The questionnaire was validated. The future work will be to test this conceptual framework to determine its influencing

relationship with largest sample of selected respondents from e-government environment in Malaysia.

REFERENCES

[1] Ihmouda R.H. and N.H. Mohd Alwi. 2013. Penetration Testing For Libyan Government Website. In: Proceedings of the 4th International Conference on Computing and Informatics, ICOCI 2013, 28-29 August, 2013. Sarawak, Malaysia. Universiti Utara Malaysia (http://www.uum.edu.my): Universiti Utara Malaysia (http://www.uum.edu.my).

[2] Ihmouda R., N.H.M. Alwi and I. Abdullah. 2014. A Systematic Review on E-government Security Aspects. International Journal of Enhanced Research in Management and Computer Applications.

[3] Smith S., R. Jamieson and D. 2007. Winchester. An action research program to improve information systems security compliance across government agencies. in System Sciences. HICSS 2007. 40th Annual Hawaii International Conference on. IEEE.

[4] Singh S. and D.S. Karaulia. 2011. E-Governance: Information Security Issues. In: International Conference on Computer Science and Information Technology (ICCSIT'2011) Pattaya.

[5] Von Solm, R. 1996. Information security management: the second generation. Computers and Security. 15(4): 281-288.

[6] Chang S.E. and C.B. Ho. 2006. Organizational factors to the effectiveness of implementing information security management. Industrial Management and Data Systems. 106(3): 345-361.

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

[8] Vermeulen C. and R. Von Solms. 2002. The information security management toolbox–taking the pain out of security management. Information Management and Computer Security. 10(3): 119-125.

[9] Dutta A. and K. McCrohan. 2002. Management's role in information security in a cyber economy. California Management Review. 45(1): 67-87.

[10] Kowalski S. 1994. IT Insecurity: A Multi-disciplinary Inquiry. Univ.

[11] Nohlberg M. 2007. Social engineering: understanding, measuring and protecting against attacks. ph. d. Licenciature, dept. Hum. And inf., univ. of skövde, Sweden.

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

[13] Kankanhalli A., *et al*. 2003. An integrative study of information systems security effectiveness. International Journal of Information Management. 23(2): 139-154.

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

[15] Da Veiga A. and J.H. Eloff. 2010. A framework and assessment instrument for information security culture. Computers and Security. 29(2): 196-207.

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

[17] Brady J.W. 2011. Securing health care: Assessing factors that affect HIPAA security compliance in academic medical centers. In System Sciences (HICSS), 2011 44th Hawaii International Conference on. IEEE.

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

[19] Veiga A.D. and J.H. Eloff. 2007. An information security governance framework. Information Systems Management. 24(4): 361-372.

[20] Ihmouda R. and N.H.M. Alwi. 2014. A Comparative Analysis of e-government security frameworks Social-Technical Security Aspect. International Journal of Management & Information Technology.

[21] Hwang M.-S., *et al*. 2014. Challenges in e-government and security of information. Information and Security: An International Journal. 15(1): 9-20.

[22] Wang J.-f. 2009. E-government security management: key factors and countermeasure. In: Proceedings of the 2009 Fifth International Conference on Information Assurance and Security-Volume 02. IEEE Computer Society.

[23] Al-Tameem A., M. Zairi and M. Kamala. 2009. Critical factors of information security implementation. In Networked Digital Technologies, 2009. NDT'09. First International Conference on. IEEE.

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

[25] AlKalbani A., H. Deng and B. Kam. 2014. A Conceptual Framework for Information Security in Public Organizations for E-Government Development. ACIS.

[26] Schlienger T. and S. Teufel. 2005. Tool supported management of information security culture, in Security and Privacy in the Age of Ubiquitous Computing. Springer. pp. 65-77.

[27] Kuusisto T. and I. Ilvonen. 2003. Information security culture in small and medium size enterprises. Frontiers of e-business Research.

[28] Ramachandran S., S.V. Rao and T. Goles. 2008. Information security cultures of four professions: a comparative study. In: Hawaii International Conference on System Sciences, Proceedings of the 41st Annual. IEEE.

[29] Tarimo C.N., *et al.* 2006. A Social-Technical View of ICT Security Issues, Trends, and Challenges: Towards a Culture of ICT Security-The Case of Tanzania. In ISSA.

[30] Alnatheer M.A. 2014. A Conceptual Model to Understand Information Security Culture. International Journal of Social Science and Humanity. 4(2).

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

[32] Al-Salihy W., J. Ann and R. Sures. 2003. Effectiveness of information systems security in IT organizations in Malaysia. In Communications, 2003. APCC 2003. The 9th Asia-Pacific Conference on. IEEE.

[33] Alfawaz S.M. 2011. Information security management: a case study of an information security culture. Queensland University of Technology.

[34] Robbins S.P. and T.A. Judge. 2012. Organizational Behavior 15th Edition. Prentice Hall.

[35] El-Haddadeh R., A. Tsohou and M. Karyda. 2012. Implementation challenges for information security awareness initiatives in e-government.

[36] Ayyagari R. and J. Tyks. 2012. Disaster at a University: A Case Study in Information Security. Journal of Information Technology Education. p. 11.

[37] Hassan N.H. and Z. Ismail. 2012. A conceptual model for investigating factors influencing information security culture in healthcare environment. Procedia-Social and Behavioral Sciences. 65: 1007-1012.

[38] Knapp K.J. and C.J. Ferrante. 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.

[39] Kraemer S. and P. Carayon. 2005. Computer and information security culture: findings from two studies. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting. SAGE Publications.

[40] A. Martins and J. Elofe. 2002. Information security culture. In Proceedings of IFIP TC11, 17th international conference on information security (SEC2002). Cairo, Egypt. Springer US.

[41] [41] Van Niekerk J. and R. von Solms. 2006. Understanding Information Security Culture: A Conceptual Framework. In ISSA.

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

[43] Knapp K.J., et al. 2007. Information security effectiveness: conceptualization and validation of a theory. International Journal of Information Security and Privacy (IJISP). 1(2): 37-60.

[44] Mishra S. and L. Chasalow. 2014. Information Security Effectiveness: A Research Framework.

[45] Sekaran U. 2003. Research methods for business: A skill building approach. John Wiley and Sons.

[46] McClendon M.J. 1994. Multiple regression and causal analysis. FE Peacock Publishers Itasca, IL.

[47] Malhotra N.K., *et al*. 2004. Essentials of marketing research: an applied orientation. Pearson Education Australia.

[48] Halit A.H. 2014. The Validity and Reliability Test for Career Intervention Program Questionnaire (CIPQ).

[49] Fraenkel J.R., N.E. Wallen and H.H. Hyun. 1993. How to design and evaluate research in education. Vol. 7. McGraw-Hill New York, USA.

[50] Creswell J.W. 2009. Research design: Qualitative, quantitative, and mixed method approaches. 3rd Ed ed. SAGE, Thousand Oaks, CA.

[51] Hair J.F., et al. 1998. Multivariate data analysis, 1998. Upper Saddle River.

[52] Nunnally J. 1978. Psychometric theory. McGraw-Hill series in Psychology.

[53] Al-Shawabkeh M., M.M. Saudi and N.H.M. Alwi. 2006. Computer security factors effects towards online usage of internet banking system. Computer. 12(36): 37.

[54] Hair J.F., et al. 2010. Multivariate data analysis, ed. S. Edition. Vol. 6. Prentice Hall, Upper Saddle River, New Jersey, USA.

[55] Fornell C. and D.F. Larcker. 1981. Evaluating structural equation models with unobservable variables and measurement error. Journal of marketing research. pp. 39-50.

[56] Chesney T. 2006. An acceptance model for useful and fun information systems. Human Technology: An Interdisciplinary Journal on Humans in ICT Environments. 2(2): 225-235.

[57] Hair J.F., et al. 2006. Multivariate data analysis. Vol. 6. Pearson Prentice Hall Upper Saddle River, NJ.

[58] Tashakkori A. and C. Teddlie. 1998. Mixed methodology: Combining qualitative and quantitative approaches. Vol. 46. Sage.