©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

COMPUTER SECURITY FACTORS EFFECTS TOWARDS ONLINE USAGE OF INTERNET BANKING SYSTEM

Mahmoud Al-Shawabkeh[1,2], Madihah Mohd Saudi[1], Najwa Hayaati Mohd Alwi[1]
[1]Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM), Nilai, Malaysia
[2]International Islamic University Malaysia (IIUM), Kuala Lumpur, Malaysia
E-Mail: mahmoud@iium.edu.my

ABSTRACT

Given an apparent lack of coherence and a paucity of computer system field of studies, research imitates and demonstrates non consensus in how computer security fits into the satisfaction, success, usage, efficiency, and effectiveness of computer system field. This study is a part of research aims to extend the Technology to Performance Chain model by including and examining the Computer Security Self-Efficacy construct, as recommend by several computer system field researchers. This paper used the statistical technique structural equation modeling and the partial least squares regression for estimating causal relations between computer security self-efficacy and internet banking usage. Outcomes confirm that confidentiality and availability effects computer security self-efficacy while in turn computer security self-efficacy impacts on usage. Computer security self-efficacy also partially mediates the impact of confidentiality, integrity, and availability on usage.

Keywords: security efficacy, online banking, computer system, social cognitive theory, task technology fit, performance impact, self-efficacy, information system, partial least squares.

INTRODUCTION

Over the years, a variety of computer system technologies is provided to customers by banking industry [1, 2, 3, 4]. Today, these technologies enable services such as online credit card management, online internet banking, and mobile banking. As anticipated, some researcher observed that banking computer systems are not used and fully utilized by some bank customers [5, 1, 6, 4. The customer's perceived lack of security is considered as an important obstacles of online internet banking growth [7]. Furthermore, the perceived security is one of the prime factors that prevent online banking adoption and usage [8]. Hence, there is a deepen need to discover, and explain the factors impacts on usage of such security related technologies [9, 10, 11, 12].

Security research generally focus on the computer technology, such as the internet voting [18], spyware and malware [13, 14, 15, 16, 17], web semantic [19], cloud computing security [20], mobile and internet banking [21]. However, computer technology security perception and effects start to be the main concern in recent studies. Difficulty of collecting data and critical nature of user secure tasks are the primary reason of having a little literature on computer system security [22, 23, 24]. In recent years, developing focused and context technology theories is an important pioneer to advance the computer system research [25, 26, 12].

For future research, there are several important directions. To extent computer system research into other established streams of research is suggested and recommended by several researchers [26, 27, 28].

Consolidating knowledge from computer system and computer security in a research model is lacking. This research paper seeks to fill this security risk gap by integrating security stream of research into another computer system dominant stream [12]. Specifically to find "to what extent has the computer security self-efficacy affected user's perception of secure computer system usage". The research objectives are:

- To explore and investigate the constructs that has impact on usage of computer system.
- To analyze and evaluate the relationship between usage of computer system and computer security self-efficacy.

The first section of this paper present literature review, which considers computer system effectiveness and computer security self-efficacy, then research framework, methodology, analysis and summary statistics, and conclusion presented in the final section.

LITERATURE REVIEW

Effectiveness of Computer System

The computer system research results that researchers have considered can be categorized as either related to performance or fit. Studies done to see if the technology usage changes users' behavior or leads to improve outcomes, or motivation are considered performance oriented. Studies which collect and analyze user' perception of how well a technology usage will help user to complete a specific task or set of tasks is defined as fit oriented.

Task-Technology-Fit is a key, but fit is often overlooked as a construct in understanding the effect of technology on user's performance [29]. The Fit is a way to measure the performance of computer systems [30]. Computer system performance can be difficult to measure; thus, the user evaluations are commonly used as the measurement. User evaluations based on the fit between task and technology has been an effective measure of

©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

computer systems performance. While researchers have carried out several studies on fit effect on performance of computer system, there is still room for further research in assessing fit and in how to best measure computer systems usage [29].

A. Social Cognitive Theory

Self-efficacy has been argued as the one of the most important factors which regulate and motivates individual behavior [31]. The social cognitive theory is concerned with how perceptions of self-efficacy affect individual's actions. According to Bandura [32], Self-efficacy is an individual belief in his abilities to mobilize the actions, motivations, and cognitive resources needed to exercise control over given events [32, 33, 34]. Self-efficacy is concerned not with the skills individual has but with judgments of what individual can do with whatever skills individual possesses. In other words, self-efficacy describes an individual's belief in his ability to perform a specific behavior. The theory is clearly well suited to studying the user's behavior in the domain of computer system, because self-regulated behavior in terms of computer systems seems critically important for ensuring the computer system's usage.

Driven from self-efficacy is computer self-efficacy (CSE) [35, 36]. Computer self-efficacy refers to self assessment of an individual's ability to practise computer skills to complete the tasks [36]. Computer self-efficacy has been related to various individual's computing behavior, such as usage and adoption of an computer system [12, 36, 37].

COMPUTER SECURITY SELF-EFFICACY

Previous research outcomes has shown that computer security self-efficacy plays a leading role in defining and using computer related applications and technologies [26, 27, 28, 31]. Based on the three computer security prime attributes, confidentiality, integrity, and availability, this study defines computer security self-efficacy as the "efficacy perceived of user ability to use computer technology to perform specific secure online task" [36, 38, 39].

PROPOSED NEW RESEARCH FRAMEWORK

In an attempt to address this paper research questions, the collected data set test with computer security self-efficacy. The base model includes three direct effects on usage, the confidentiality, integrity, and availability. The relationship between technology to computer self-efficacy and usage was tested by previous research [40] in which the finding was that computer self-efficacy has a direct effect on performance, but no significant interaction effects. This research however, intends to test model on online banking context that have tasks with security characteristics. The relationship between confidentiality, integrity, availability and usage need to be tested. The analysis then tests the additions of the computer security self-efficacy (CSSE) construct as both a direct effect and a mediator with confidentiality, integrity, and availability. Figure-1 shows the new proposed framework. The framework hypothesis is shown in Table-1. Constructs definitions are shown in Table-2.

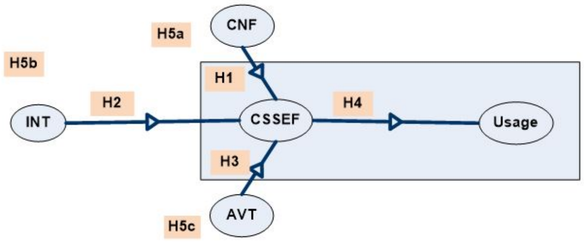

Figure-1. Research framework (New model of computer security).

Table-1. Research hypothesis.

H1	**Confidentiality positively impacts on computer security self-efficacy**
H2	Integrity positively impacts on computer security self-efficacy.
H3	Availability positively impacts on computer security self-efficacy.
H4	Computer security self-efficacy positively impacts on usage.
H5a	Relationship between confidentiality and usage is moderated by computer security self-efficacy
H5b	Relationship between integrity and usage is moderated by computer security self-efficacy
H5c	Relationship between availability and usage is moderated by computer security self-efficacy

Table-2. Construct definitions.

Construct	Definition
(CNF) Confidentiality	Confidentiality prevents disclosure of computer to unauthorized person by ensuring that computer is accessible only by authorized users.
(INI) Integrity	Integrity is the ability of the computer system to prevent unauthorized modification or deletion of data. Integrity in general refers to the data validity.
(AVT) Availability	Availability of the system refers to perform its stated function at a specific instant of time or over a stated period of time.
(CSSE) Computer security self-efficacy	Efficacy perceived of user ability to use computer technology to perform specific secure online task.
(SU) System usage	Usage can be influenced by the process of confidentiality, integrity, availability, and the fit between them.

©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

RESEARCH METHODOLOGY

A multi-method approach was chosen since it facilitates explanation and prediction as well as assisting in developing a more holistic view of the aspects under investigation [41]. Computer security experts and academics were interviewed to support literature and develop survey questions related to the computer security self-efficacy. To validate the questionnaire, a survey feasibility was carried out in pervious pilot study [42]. After that, the quantitative research method used for current research data collection. Table-3 shows the research constructs sources. This study unit of analysis is all internet users in Klang Valley area, Malaysia [43].

Table-3. Constructs sources.

Constructs	Sources
(CNF) Confidentiality	[1], [44], [45], [46], [47]
(INI) Integrity	[1], [44], [45], [46], [47]
(AVT) Availability	[1], [44], [45], [46], [47]
Computer Security Self Efficacy	Literature+ Interview [39], [36], [33], [32], [34], [48], [49], [50], [51], [52], [28], [12], [27], [26], [31], [32, 33], [40], [53] Main Source: [54]
System Usage	[40], [55], [56], [57], [58], [29], [59], [60], [61] Main Source: [56]

A. Data collection

A period of three months was carried out during the process of distribution and collection of One Thousand self-administered survey questionnaires. In this paper analysis, a total of 302 questionnaires were used which translates about 30% response rate.

B. Goodness measures and assessment

A 5-point Likert scale was used to collect data for each construct of this research. For the proposed model constructs, this research developed the questionnaire items by choosing constructs found in previous researches [56], [62], [40], [63], [64]. Validity and reliability are the two criteria used to test measures goodness [65].

C. Construct validity

Convergent and discriminant validity used to measure construct validity [65]. Cross loading and loading, both recommended for determining problems with any particular survey item. As shown in Table-4, a value of loadings at 0.5 was used as a significant [43]. Results shows that all items measuring construct loaded lower on the other constructs and loaded highly on that particular construct. This confirmed the construct validity.

Table-4. Loadings and cross loadings.

	CSSE	CNF	INT	AVT	US
CSSE1	0.75	0.18	0.25	0.27	0.13
CSSE2	0.77	0.35	0.29	0.47	0.19
CSSE3	0.74	0.38	0.32	0.45	0.25
CSSE4	0.77	0.17	0.25	0.25	0.09
CSSE5	0.81	0.25	0.31	0.3	0.1
CSSE6	0.78	0.31	0.24	0.34	0.18
CSSE7	0.82	0.37	0.27	0.4	0.17
CSSE8	0.86	0.34	0.27	0.4	0.13
CSSE9	0.87	0.25	0.25	0.3	0.13
CSSE10	0.73	0.33	0.32	0.36	0.22
CSSE11	0.72	0.27	0.22	0.36	0.13
CSSE12	0.73	0.2	0.29	0.31	0.09
CSSE13	0.74	0.13	0.14	0.22	-0.06
CSSE14	0.77	0.23	0.17	0.31	-0.02
CNF1	0.37	0.92	0.6	0.8	0.54
CNF2	0.36	0.88	0.6	0.77	0.56
CNF3	0.32	0.9	0.6	0.73	0.53
CNF4	0.33	0.9	0.61	0.75	0.53
CNF5	0.27	0.88	0.61	0.7	0.52
CNF6	0.26	0.75	0.58	0.51	0.54
CNF7	0.28	0.87	0.62	0.69	0.63
INT1	0.25	0.56	0.89	0.49	0.62
INT2	0.35	0.67	0.89	0.62	0.58
INT3	0.27	0.64	0.85	0.57	0.56
INT4	0.38	0.57	0.85	0.53	0.53
INT5	0.26	0.62	0.88	0.52	0.59
INT6	0.24	0.56	0.85	0.44	0.5
INT7	0.28	0.5	0.78	0.41	0.46
AVI1	0.38	0.73	0.61	0.87	0.44
AVI2	0.33	0.65	0.51	0.82	0.35
AVI3	0.45	0.63	0.41	0.81	0.37
AVI4	0.41	0.69	0.41	0.88	0.42
AVI5	0.4	0.69	0.46	0.86	0.43
AVI6	0.35	0.66	0.47	0.85	0.39
AVI7	0.36	0.78	0.66	0.85	0.59
SU1	0.16	0.53	0.61	0.45	0.9
SU2	0.12	0.48	0.48	0.42	0.83
SU3	0.17	0.56	0.52	0.41	0.8

D. Convergent validity

In this research, to measure convergence validity the average variance extracted, composite reliability, and factor loadings were used [43].

As shown in Table-5, results confirmed factor loading by shown all items loadings exceeded the recommended value of 0.5. As well as shown that composite reliability values ranged from 0.88 to 0.96. Composite reliability describes the degree to which the construct indicators indicate the latent. Composite reliability usually confirmed when exceeded the recommended value of 0.7 [43].

Table-5. Meacurement model results.

	AVE	Composite reliability	R^2	Cronbachs Alpha
CSSE	0.6	0.95		0.95
CNF	0.76	0.96	0.67	0.95
INT	0.73	0.95	0.47	0.94
AVT	0.72	0.95	0.46	0.93
US	0.71	0.88		0.79
CR = $(\sum \text{standardized loading i})^2 / (\sum \text{ loading i})^2+(\Sigma \epsilon i)^2$ $R^2 = (\sum \text{standardized loading i}^2) / (\sum \text{loading i}^2) + \Sigma \epsilon i^2)$ "Where e is errors" [43].				

The measures of the variance captured by the indicators relative to measurement error is the average variance extracted (AVE), value of 0.5 or above will justify using a construct average variance extracted [66]. The results shows range of 0.60 and 0.72 is the average variance extracted as shown in Table-6. Based on the statistical significance and parameter estimates, the results show that all constructs confidentiality, integrity, availability, computer security self-efficacy and usage are all valid measures of their respective constructs [67].

Table-6. M model results (Loading and T value).

Construct	Latent	Original sample (O)	T Statistics (|O/STERR|)
CSSE	CSSE1	0.745	7.7316
	CSSE2	0.7656	10.4832
	CSSE3	0.738	8.7298
	CSSE4	0.7749	7.8183
	CSSE5	0.8103	9.8299
	CSSE6	0.7844	10.6903
	CSSE7	0.8238	13.0648
	CSSE8	0.8648	15.3584
	CSSE9	0.8653	13.5191
	CSSE10	0.7272	7.3494
	CSSE11	0.7161	7.7093
	CSSE12	0.7309	7.6533
	CSSE13	0.7406	7.7739
	CSSE14	0.7666	8.8679
CNF	CNF1	0.9182	42.3939
	CNF2	0.8785	20.4884
	CNF3	0.9048	26.7024
	CNF4	0.8968	22.3719
	CNF5	0.879	20.9216
	CNF6	0.746	5.5828
	CNF7	0.8663	20.6325
INT	INT1	0.8924	25.8179
	INT2	0.8868	29.9587
	INT3	0.8545	18.8941
	INT4	0.8511	12.1505
	INT5	0.8783	19.8471
	INT6	0.85	15.0615
	INT7	0.7821	8.4663
AVT	AVT1	0.8658	21.9366
	AVT2	0.8153	14.3107
	AVT3	0.815	14.2323
	AVT4	0.8769	15.6257
	AVT5	0.8601	14.9867
	AVT6	0.8522	12.8333
	AVT7	0.8457	15.5532
US	SU1	0.8964	31.0311
	SU2	0.8288	10.2957
	SU3	0.7956	12.0581

E. Discriminant validity

The potentially overlapping constructs correlations were measured by constructs discriminant validity. As shown in Table-7, adequate discriminant validity confirmed by the squared correlations for each construct is less than the average variance extracted by the indicators measuring that construct.

Table-7. Constructs discriminate validity.

	CSSE	CNF	INT	AVI	US
CSSE	**0.77**				
CNF	0.36	**0.87**			
INT	0.34	0.69	**0.85**		
AVI	0.45	0.82	0.6	**0.85**	
SU	0.18	0.63	0.64	0.51	**0.84**

F. Reliability analysis

Loadings and alpha values are summarized in Table-8. The inter item consistency was measured by

Cronbach's alpha coefficient. Results shows all Cronbach's alpha values are above 0.60 [68]. The value 0.7 or greater of Composite reliability considered acceptable [69]. The results shows composite reliability values ranged from 0.88 to 0.96. This concluded the measurements reliability

Table-8. Reliability test results.

	Cronbachs Alpha	Loading range	Num item
CSSE	0.95	0.72-0.87	14(14)
CNF	0.95	0.75-0.92	7(7)
INT	0.94	0.78-0.89	7(7)
AVI	0.93	0.81-0.88	7(7)
SU	0.79	0.80-0.90	3(3)

G. Hypotheses testing

For the path analysis, all hypotheses generated were tested. Figure-2 shows the framework and Table-9 presents statistical results. The R^2 value was 0.336 suggesting that 33.6% of the variance in extent of computer security self-efficacy can be explained by variables confidentiality, integrity, and availability. Hypotheses H1, H3, and H4 of the study were supported, whereas the hypotheses H2 not supported.

Sobel statistical test used to measure the mediation effect of computer security self-efficacy, Sobel statistical test measure whether computer security self-efficacy significantly influence all other variables. Results indicate that computer security self-efficacy mediates the relationships between confidentiality, availability and usage. The results provide support for H5a and H5c.

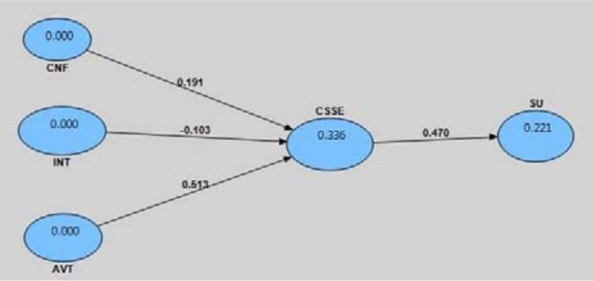

Figure-2. Path analysis result.

Table-9. Hypothesis testing and Path coefficients.

	Relationships	Supported	Coefficients	t value
H1	CNF->CSSE	Yes	0.191	3.0367
H2	INT->CSSE	No	-0.103	2.4993
H3	AVI->CSSE	Yes	0.513	3.817
H4	CSSE->SU	Yes	0.470	4.140
H5a	CNF->CSSE->SU	Yes		2.340
H5b	INT->CSSE->SU	No		0.177
H5c	AVI->CSSE->SU	Yes		2.601

CONCLUSIONS

This research paper has developed and validated a questionnaire for measuring effects of computer security factors on the usage of online banking. For future work, the findings for this paper can be further explored and can be used as a basis for further study in different scope such as in social networks and cloud computing. Furthermore, different regional interdependency analysis might produce a different result. Previous studies have demonstrated that regional interdependence is an important consideration. For example, rural areas in Japan can be relatively less secure than urban areas [70].

ACKNOWLEDGEMENTS

The authors would like to express their gratitude to Universiti Sains Islam Malaysia (USIM), Centre for Foundation Studies, International Islamic University Malaysia and Institut Sains Islam (ISI), USIM for the support and facilities provided. This research paper is supported by Universiti Sains Islam Malaysia (USIM) grant [PPP/FST/SKTS/30/12712] and [PPP/FST/SKTS/30/12812].

REFERENCES

[1] S. Chan and M. Lu. 2004. Understanding internet banking adoption and use behavior: A Hong Kong perspective. Journal of Global Information Management. 12: 21.

[2] V. S. Lai and H. Li. 2005. Technology Acceptance Model for Internet Banking: An invariance Analysis. Information and Management. 42: 13.

[3] A. Sachan and A. Ali. 2006. Competing in the age of information technology in a developing economy: Experiences of an Indian Bank. Journal of Cases on Information Technology. 8: 19.

[4] W. Wresch and S. Fraser. 2006. Managerial strategies used to overcome technological hurdles: A review of e-commerce efforts used by innovative Caribbean managers. Journal of Global Information Management. 14: 16.

[5] J. A. Cazier, B. M. Benjamin and R. D. Louis. 2006. E-business differentiation through value-based trust. Information and Management. 43: 9.

[6] Y. S. Wang, Y. M. Wang, H. H. Lin and T. I. Tang. 2003. Determinants of user acceptance of internet banking: An empirical study. International Journal of Service Industry Management. 14: 18.

[7] Thorton Consulting. 1996. Thorton consulting online banking: a success. Australian Banking and Finance. vol. 5.

[8] B. Howcroft, R. Hamilton and P. Heder. 2002. Consumer attitude and the usage and adoption of home-based banking in the United Kingdom. International Journal of Bank Marketing. 20: 10.

[9] H. Amin. 2007. Internet banking adoption among young intellectuals. Journal of Internet Banking and Commerce. 12: 13.

[10] D. R. Compeau, C. A. Higgins and S. Huff. 1999. Social cognitive theory and individual reaction to computing technology: A longitudinal study. MIS Quarterly. MIS Quarterly. 23: 13.

[11] F. D. Davis, R. P. Bagozzi and P. R. Warshaw. 1989. User acceptance of computer technology: A comparison of two theoretical models. Management Science. 35: 19.

[12] V. Venkatesh, M. G. Morris, G. B. Davis and F. D. Davis. 2003. User acceptance of information technology: Toward a unified view. MIS Quarterly. 27: 425-478.

[13] M. M. Saudi. 2011. A NEW MODEL FOR WORM DETECTION AND RESPONSE. PhD, Department of Computing, School of Computing. Informatics and Media, University of Bradford.

[14] M. M. Saudi, A. J. Cullen and M. Woodward. 2011. Efficient STAKCERT KDD Processes in Worm Detection. World Academy of Science, Engineering and Technology Journal. p. 3.

[15] Lee and Kozar. 2005. Investigating Factors Affecting the Adopting of Anti-Spyware Systems. Communications of ACM. 48: 5.

[16] Zang. 2005. What do Consumers Really Know about Spyware? Communications of ACM. 48: 4.

[17] R. Power. 2008. CSI computer crime and security survey. Computer Security Institute.

[18] Jefferson Rubin, Simons and Wagner. 2004. Analyzing Internet Voting Security. Communications of the ACM. 47: 5.

[19] Lee Shambhu, Raghav and Sharman. 2005. Secure Knowledhe Management and The Semantic Web. Communications of the ACM. 48: 6.

[20] D. Zissis and D. Lekkas. 2012. Addressing cloud computing security issues. Future Generation Computer Systems. 28: 9.

[21] Gimun Kim, BongSik Shin and H. G. Lee. 2009. Understanding dynamics between initial trust and usage intentions of mobile banking. Information Systems Journal. 19: 28.

[22] Hong Kwo-Shing, Chi Yen-Ping, Chao Louis, et al. 2003. An Integrated System Theory of Information Security Management. Information Management and Computer Security. vol. 11.

[23] Kotulic Andrew and Clark. 2004. Why there aren't more information security research studies. Information and Management. 41: 13.

[24] C. Sherrie, C. P. Prashant and S. Richard. 2006. A Research Framework for Information Systems Security. Journal of Information Privacy and Security. 2: 27.

[25] W. Orlikowski and C. Iacono. 2001. Research Commentary: Desperately Seeking the "IT" in IT Research-A Call to Theorizing the IT Artifact. Information System Research. 12: 121-134.

[26] V. Venkatesh and H. Bala. 2008. Technology Acceptance Model 3 and a Research Agenda on Interventions. Decision Sciences. vol. 39.

[27] S. A. Brown, A. R. Dennis and V. Venkatesh. 2010. Predicting Collaboration Technology Use: Integrating Technology Adoption and Collaboration Research. Journal of Management Information Systems. 27: 9-53, Fal.

[28] A. R. Dennis, V. Venkatesh and V. Ramesh. 2003. Adoption of Collaboration Technologies: Integrating Technology Acceptance and Collaboration Technology Research. Working Papers on Information Systems. vol. 3.

[29] D. L. Goodhue. 1995. Understanding User Evaluations of Information Systems. Management Science. 41: 17.

[30] M. L. Irick. 2008. Task-technology fit and information systems effectiveness. Journal of Knowledge Management Practice. vol. 9.

[31] A. Bandura and F. Jourden. 1991. Self-regulatory mechanisms governing the impact of social comparison on complex decision making. Journal of Personality and Social Psychology. 60: 10.

[32] A. Bandura. 1986. Social foundations of thoughts and action: a social cognitive theory. Englewood Cliffs: Prentice Hall.

[33] A. Bandura. 1997. Self-efficacy: The exercise of control. New York: Freeman.

[34] E. Ozer and A. Bandura. 1990. Mechanisms governing empowerment effects: a self-efficacy analysis. Journal of Personality and Social Psychology. 58: 14.

[35] F. Davis and P. Warshaw. 1989. User acceptance of computer technology: A comparison of two theoretical models. Management Science. 35: 982-1103.

[36] D. Compeau and C. Higgins. 1995. Computer self-efficacy: development of a measure and initial test. MIS Quarterly. 19: 12.

[37] P. Ellen, W. Bearden and S. Sharma. 1991. Resistance to technological innovations: an examination of the role of self-efficacy and performance satisfaction. Journal of the Academy of Marketing Science. 19: 10.

[38] M. Smith. 1989. Computer security-threats, vulnerabilities, and countermeasures. Information Age. 11: 5.

[39] G. Marakas, M. Yi and R. Johnson. 1998. The multilevel and multifaceted characteristics of computer self-efficacy. Information Systems Research. 9: 26.

[40] D. M. Strong, M. T. Dishaw and D. B. Bandy. 2006. Extending Task Technology Fit with Computer Self-Efficacy. Database for Advances in Information Systems. 37: 96-107.

[41] L. Bradley and K. Stewart. 2003. The diffusion of online banking. Journal of Marketing Management Information Systems Quarterly. 19: 22.

[42] Mahmoud, Madihah and Najwa. 2012. Computer Security Self-Efficacy Factors Influencing E-Banking Utilization and User Satisfaction. Presented at the Seminar Hasil Penyelidikan, Kementerian Pengajian Tinggi, Akademi Kepimpinan Pengajian Tinggi (AKEPT) Lebuh Enstek, Bandar Enstek, Negeri Sembilan.

[43] B. W. Hair JF, Babin BJ, Anderson RE. 2010. Multivariate data analysis. Upper Saddle River: Prentice-Hall.

[44] F. Sattarova and K. Tao-hoon. 2007. IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. International Journal of Multimedia and Ubiquitous Engineering. Vol. 2

[45] D. B. Parker. 1998. Fighting Computer Crime. New York: Wiley Publishing.

[46] M. Hayes. 2002. Where The Chief Security Officer Belongs. Information Week.

[47] P. Toal. 2011. Oracle White Paper - Information Security: A Conceptual Architecture Approach.

[48] N. E. Miller and J. Dollard. 1941. Social Learning and Imitation. New Haven, CT: Yale University Press.

[49] A. Bandura and R. H. Walters. 1963. Social Learning and Personality Development. New York: Holt, Rinehart and Winston.

[50] K. Glanz, B. K. Rimer and F. M. Lewis. 2002. Health Behavior and Health Education. Theory, Research and Practice. San Fransisco: Wiley and Sons.

[51] A. Bandura. 2001. Social cognitive theory: An agentive perspective. Annual Review of Psychology. 52: 26.

[52] V. Venkatesh, C. Speier and M. G. Morris. 2002. User acceptance enablers in individual decision making about technology: Toward an integrated model. Decision Sciences. 33: 297-316.

[53] D. Compeau, J. Gravill, N. Haggerty and H. Kelley. 2006. Computer self efficacy: a review. In: Zhang P, Galletta D, editors. in computer interaction and management information systems.

[54] R. Hyeun-Suk, K. Cheongtag and U. R. Young. 2009. Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers and Security. 28: 10.

[55] N. Venkatraman. 1989. The Concept of Fit in Strategy Research: Toward Verbal and Statistical Correspondence. Academy of Management Review. 14: 423-444.

[56] D. L. Goodhue and R. L. Thompson. 1995. Task-Technology Fit and Individual-Performance. MIS Quarterly. 19: 213-236.

[57] D. L. Goodhue. 1988. Supporting users of corporate data: the effect of I/S policy choices. Ph D,

Massachusetts Institute of Technology, Sloan School of Management.

[58] D. L. Goodhue. 1998. Development and measurement validity of a task-technology fit instrument for user evaluations of information systems. Decision Sciences. 29: 34.

[59] D. L. Goodhue. 1992. User evaluations of MIS success: What are we really measuring? In Proceedings of the Hawaii Twenty-Fifth International Conference on Systems Sciences. pp. 303-314.

[60] D. Goodhue, R. Littlefield and D. Straub. 1997. The Measurement of the Impacts of the IIC on the End-Users: The Survey. Journal of the American Society for Information Science. 48: 12.

[61] D. Goodhue. 1997. The model underlying the measurement of the impacts of the IIC on the end-users. Journal of the American Society for Information Science. 48: 449-453.

[62] M. T. Dishaw and D. M. Strong. 1998. Assessing software maintenance tool utilization using task-technology fit and fitness-for-use models. Journal of Software Maintenance-Research and Practice. 10: 151-179.

[63] M. T. Dishaw and D. M. Strong. 2003. The Effect of Task and Tool Experience on Maintenance CASE Tool Usage. Information Resources Management Journal. 16: 1-16.

[64] M. T. Dishaw and D. M. Strong. 1998. Supporting Software Maintenance with Software Engineering Tools: A Computed Task-Technology Fit Analysis. The Journal of Systems and Software. 44: 107-120.

[65] U. Sekaran and R. Bougie, Research Methods for Business - A Skill Building Approach, 5th Edition ed. Chichester: John Wiley & Sons, 2010.

[66] T. R. Barclay DW, Higgins C. 1995. The partial least squares (PLS) approach to causal modeling: personal computer adoption and use an illustration. Technol Stud. 2: 285-309.

[67] C. L. Chow WS. 2008. Social network and shared goals in organizational knowledge sharing. Information Management. 45: 24-30.

[68] B. I. Nunnally J, 1994. Psychometric Theory. New York: McGraw-Hill.

[69] L. D. Fornell C. 1981. Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research. 18: 39-50.

[70] H. Tanaka. 2009. Quantitative Analysis of Information Security Interdependency between Industrial Sectors. Presented at the Third International Symposium on Empirical Software Engineering and Measurement.