International Journal of Science and Engineering Applications
Volume 4 Issue 6, 2015, ISSN-2319-7560 (Online)

Mediating role of Information System Security Awareness in the relationship between Self-Efficacy, Security Practice and Information System Security Behavior

Hanieh Yaghoobi Bojmaeh
London Metropolitan University
London,United Kingdom

Abstract: Through reviewing the previous conducted studies, we can find enough evidence in order to support the relationship between self-efficacy and security practice with information system security behavior. The main issue which is discussed in this research is the key role of information system security awareness. According to the data analysis results on 230 collected data from 10 universities in Iran, located in Tehran, it was revealed that the relationship between mentioned factors with information system security can be mediated by information system security awareness

Keywords: Self-Efficacy, Security Practice, Information System Security Behavior, Information System Security Awareness

1. INTRODUCTION

In fact, security awareness is the attitude and knowledge of organizational members toward the protection of informational as well as physical organizational assets. Many firms need to have some formal security awareness education programs for all of their staffs while they are being employed in organization and thereafter periodically, mainly annually.
Still, information system security is a challenging issue for executives and professionals. A lot of investigations on this topic are technical in nature and so would not focus on individual and organizational issues. Currently, unfortunately, a lot of companies do not have sufficient emphasize on individual values, thus, they just focus on technical aspects. Due to human errors and technical errors, firms should be aware about importance of training responsible workers for reinforcing the IS security. In this paper, ICT departments of many Iranian universities have been selected as scope of study. It demonstrates that this research puts effort to recognize the main influential factors which impact IS security behavior within the Iranian universities.
However, this research believes that some factors such as self-efficacy and security practices (technology and care behavior), at first will increase IS security and then impact the IS security behavior. The influence of self-efficacy and also security practices on awareness and behavior in ICT universities of Iran is an important subject which should be studied exactly. Therefore, this study aims to find how IS security awareness affects the relationship between self-efficacy, security practices and IS security behavior.

2. LITERATURE REVIEW

The information security management in an organization includes a set of actions which have both technical and organizational implications. For example, establishing an IS security management system according to ISO/IEC 270001 (ISO, 2005), standard, involves those actions that impact organizational structure, introducing processes and policies, practices and change responsibilities as well as introducing defined technical and functional specification. One of the critical practices of any type of IS security management system is awareness of information security. Joining different methods together, security awareness could be explained as a continuous attempt of raising the attention of audiences into importance of information security for stimulating the security-oriented behaviors (Peltier, 2005; European Network and Information Security Agency (ENISA, 2008).
Previous conducted studies by (CSI, 2009; Ernst and Young, 2008; BEER, 2008), demonstrate the importance of awareness actions revealing that a main part of security losses are the results of non-malicious, totally careless behaviors of the insiders as well as the fact that security has a key role in developing a strategic perspective of information security.
The survey conducted by Ernst and Young (2010), asserts that a lot of existed security awareness and training programs are not functioning well as they can be.
According to the Computer and Crime Security Survey (CSI, 2009), the longest continuous survey running in field of IS, almost 43.4% of participants noted that less than 1% of their total security budget was devoted to awareness training programs. It seems logical to assume that effective trainings on awareness usually are less costly than security technology armory which is used by most of the companies to apply defense appropriately. Also, 55% of participants mentioned that the made investment on such training programs was not efficient. Similar phenomenon occurred in 2008 CSI Computer Crime and Security Survey (CSI, 2008). There it was found that little amount of money has been pushed toward efforts of information security awareness. It is not east to explain why these amounts are lower than some discussions about necessity of security awareness training programs may offer (CSI, 2008, P.9).

2.1. Approaches to IS system Awareness

Most of the frameworks of IS awareness offer or implement some awareness approaches and methods, for example techniques for conveying security messages, computer games, artificial intelligence devices, etc., with no justification of

their specific choices and also defining their theoretical foundations (Tsohou et al., 2008; Puhakainen, 2006). In addition, those research methods which are in nature theoretical and test the problems and challenges of security awareness, exclusively draw from behavioral and physical theories. However, these behavioral and psychological theories are not capable of mentioning organizational and social dimensions of security awareness appropriately, therefore, cannot offer a perspective on the direction of this process in an organizational environment and demonstrate those events which result in specific consequences.

In addition, Thomas and von Solms (1998) referred to social psychological theories and used psychological rules for developing an effective security awareness program. They defined an attitude system that based on it the attitude of a user can be impacted by behavior cognitions, behavior intentions as well as affective responses. In this regard, scholars concentrated on three approaches which can impact attitude of a person via persuasion: the first approach is changing their behavior directly; second is employing a change in behavior for impacting the attitude of a person and lastly changing the attitude of a person by means of persuasion and also offer a series of psychological techniques and rules in order to change the overall attitude of a person. Siponen (2000) suggested a conceptual foundation regarding security awareness based on theories of planned behavior, reasoned action, technology acceptance model and intrinsic motivation.

According to mentioned points above, Siponen (2000), presents practical principles and approach with respect to motivation: emotions, logic, ethics and morals, rationality, feeling of security and well being.

Also, Qing et al., (2007) used model of elaboration likelihood as their framework for recognizing the degree of effectiveness of persuasive communications. They reviewed effectiveness of security messages and also impacts of various messages related to modifying behavior of recipients. Besides, Puhakainen 92006) investigated on behavioral changes and compliance of IS users with information system security, instructions and policies through employing instructional and attitudinal theories. D' Archy et al., (2009) tested the counter measures of security awareness from a general perspective of deterrence theory and studied how security policy awareness, security awareness, education and theory programs as well as computer monitoring are related to misuse intention of IS.

Even though research methods to security awareness are limited in social and managerial perspectives, Spears and Barki (2010), recently, in their study examined participation of users in information system security risk management and also its impact in field of regulatory compliance. Based on their research, participation of users in security risk management helps to better organizational awareness of IS security.

Many scholars (Karamizadeh et al., 2013; Rhee et al., 2009; Richardson, 2007; Proctor et al., 2006; Lee and Kozar, 2005) have demonstrated various variables that have a high potential to impact information security behavior. These variables include, self-efficacy, security practices (care behavior, technology) and also IT practice intention. It would be efficient if this study only measures self-efficacy, security practices and care behavior. Because according to technology acceptance model, intention has the capability to generate behavior. However, this study focuses on intervening role of IS system awareness. Figure 1 illustrates the proposed framework of this research.

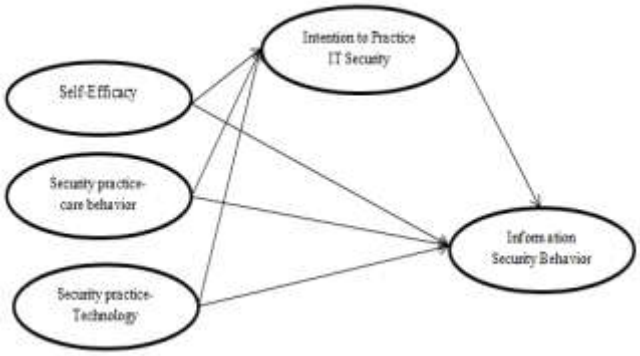

Figure 1: Proposed framework of this study

3. Methodology and Results

At the first this study developed 10 hypotheses as follow:

H1: IS security awareness is affected by self-efficacy significantly

H2: IS security awareness is affected by security practice-care behavior significantly

H3: IS security awareness is affected by security practice-technology significantly

H4: IS security behavior is affected by self-efficacy significantly

H5: IS security behavior is affected by security practice-care behavior significantly

H6: IS security behavior is affected by security practice-technology significantly

H7: IS security behavior is affected by security awareness significantly

H8: IS security awareness mediates the relationship between self-efficacy and IS security behavior

H9: IS security awareness mediates the relationship between security practice-care behaviorand IS security behavior

H10: IS security awareness mediates the relationship between security practice-care behaviorand IS security behavior

In order to evaluate all of the underlying elements of this research, the designed questionnaire by Karamizadeh et al., (2013) was utilized. Based on their study, self-efficacy includes two main aspects known as computing behavior and IT knowledge. Having intention to practice security of IT can be evaluated by security measures and IT literacy. The concept of security practice-care behavior means sharing files online and also data protection. In addition, security practice-technology means spam and antivirus filtering. Moreover, in order to measure IS security awareness; we used the conducted studies by Tshou et al., (2012).

The population of this research is all of the employees (technicians, engineers and managers) who are working in ICT departments in 10 large Iranian universities. Sample size was equal to 230. Also, the reliability test results demonstrated that all of the factors have excellent or good internal consistency. To examine the formulated hypotheses, first we applied the Pearson Correlation test.

The outcome of the Pearson correlation test showed that all independent variables have significant relationship with IS security awareness and IS behavior. The highest correlation with IS security awareness refers to security practice-care behavior while the lowest refers efficacy. The results were inverse for IS security behavior. Besides, the relationship between IS security awareness and IS security behavior was significant (.723).

The result of regression analysis shows that 72.3 percent of variation of information security behavior can be accounted

by the four existing independent variables because R square is equal to .723.
Table 1 demonstrates the results of first multiple regression analysis of this study:

Table1: Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	T	Sig	Tolerance	VIF
1	(Constant)	1.480	.333		4.438	.000		
	SELFEFF	.153	.068	.143	2.260	.025	.999	1.001
	SECCARE	.226	.070	.207	3.207	.002	.961	1.040
	SECTECH	.156	.066	.152	2.365	.019	.962	1.040

a. Dependent Variable: ISAwarness

The estimated R-square for the first regression analysis was equal to .659. In other words, 65.9% of variation of IS security awareness can be accounted by self-efficacy, security practice-care behavior, and security practice-technology. As shown in table 1, all variables (self-efficacy, security practice-care behavior, and security practice-technology) have significant impacts on IS security awareness. Henc, H1, H2, and H3 are supported by this study. The results of this regression can be written as following equation:

IS security awareness= 1.48+ .153 (Self-Eff)+ .226 (SEC-CARE)+ .156 (SEC-TECH)

Table2: Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	T	Sig.	Tolerance	VIF
1	(Constant)	1.113	.325		3.426	.001		
	SELFEFF	.142	.066	.132	2.165	.031	.999	1.001
	SECCARE	.330	.068	.307	4.844	.000	.961	1.040
	SECTECH	.178	.065	.171	2.754	.006	.962	1.040

a. Dependent Variable: ISBEHA

The estimated R-square for the second regression analysis was equal to .754. In other words, 75.4% of variation of IS security behavior can be accounted by self-efficacy, security practice-care behavior, and security practice-technology. As shown in table 2, all variables (self-efficacy, security practice-care behavior, and security practice-technology) have significant impacts on IS security behavior. Henc, H4, H5, and H6 are supported by this study. The results of this regression can be written as following equation:

IS security behavior= 1.13+ .142 (Self-Eff)+.339 (SEC-CARE)+.178 (SEC-TECH)

Table3: Coefficient

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	.434	.115		3.760	.000
	ISsecurity Awareness	.857	.035	.848	24.203	.000

a. Dependent Variable: ISBEHA

The estimated R-square for the third regression analysis was equal to .821. In other words, 82.1% of variation of IS security behavior can be accounted by IS security awareness. As shown in table 3, IS security awarenesson IS security behavior. Hence, H7 is supported by this study. The results of this regression can be written as following equation:

IS security behavior= .434+ .857(IS security behavior)

Table 4: Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	T	Sig.	Tolerance	VIF
1	(Constant)	2.633	.226		11.579	.000		
	SELFEFF	.133	.071	.127	1.880	.000	1.000	1.000
2	(Constant)	.411	.132		3.100	.000		
	SELFEFF	.008	.038	.008	.217	.828	.980	1.020
	ISAwarness	.858	.036	.847	23.883	.000	.980	1.020

a. Dependent Variable: ISBEHA

According to the table 4, in the first regression analysis self – efficacy has a significant impact on IS security behavior (p-value is equal to zero which is less than .05). In the second regression self- efficacy does not have significant impact on IS security behavior while the impact of IS security awareness is significant. So, IS security awareness fully mediates the relationship between self-efficacy and IS security behavior. Therefore, H8 is accepted by this study.

Table 5: Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	1.961	.212		9.238	.000		
	SECCARE	.372	.069	.338	5.418	.000	1.000	1.000
2	(Constant)	.062	.141		.441	.660		
	SECCARE	.106	.048	.148	4.428	.000	.940	1.064
	ISAwarness	.822	.033	.814	25.412	.000	.940	1.064

a. Dependent Variable: ISBEHA

According to the table 5, in the both regression analyses security practice-care behavior have significant impacts on IS security behavior (p-value is equal to zero which is less than .05). So, IS security awareness partially mediates the relationship between security practice-care behavior and IS security behavior. Therefore, H9 is accepted by this study.

Table 6: Coefficients[a]

Model		Unstandardised Coefficients		Standardised Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	1.313	.206		11.411	.000		
	SECTECH	.272	.067	.232	3.605	.000	1.000	1.000
2	(Constant)	.703	.142		4.948	.000		
	SECTECH	.074	.037	.071	1.995	.047	.963	1.039
	ISAwareness	.343	.034	.335	21.515	.000	.963	1.039

a. Dependent Variable: ISBEHA

According to the table 6, in the both regression analyses security practice-technology have significant impacts on IS security behavior (p-value is equal to zero which is less than .05). So, IS security awareness partially mediates the relationship between security practice-technology and IS security behavior. Therefore, H10 is accepted by this study.

3. CONCLUSION AND DISCUSSION

The achieved outcomes revealed that all of the mentioned elements have a remarkable impact on IS behavior and also information system security awareness. Moreover, IS security awareness can mediate the relationship between dependent and independent factors. Therefore, ICT departments in universities of Iran could improve such factors for reinforcing the awareness and IS security behavior. The future investigations can examine the developed framework of this research in other scopes too. Besides, the R-Square amount in current research is not high, therefore, it can be possible that other elements also can be added to this developed framework.

4. REFERENCES

[1] BERR (2008), "Information Security Breaches Survey", technical report, PricewaterhouseCoopers, in association with Symantec, HP and The Security Company, available at: www.pwc.co.uk/pdf/BERR_ISBS_2008(sml).pdf (accessed October 10, 2010).

[2] Computer Security Institute (CSI) (2008), "Computer Crime and Security Survey 2008", Computer Security Institute, available at: http://www.cse.msstate.edu/Bcse6243/readings/CSIsurvey2008.pdf (accessed July 5, 2012).

[3] D'Archy, J., Hovav, A. and Galletta, D. (2009), "User awareness of security countermeasures and its impact on information security misuse: a deterrence approach", Information Systems Research, Vol. 20 No. 1, pp. 79-98.

[4] Ernst & Young (2008), "Annual Global Information Security Survey", available at: www.arc-tc. com/pages/documents/ErnstandYoung2008.pdf (accessed February 9, 2011).

[5] Ernst & Young (2010), "12th Annual Global Information Security Survey: outpacing change", available at: www.ey.com/Publication/vwLUAssets/12th_annual_GISS_pub/$FILE/ 12th_annual_GISS_AU0383.pdf (accessed February 9, 2011).

[6] European Network and Information Security Agency (ENISA) (2008), "A new users' guide: how to raise information security awareness", ENISA, Heraklion, available at: www.enisa.europa.eu/doc/pdf/deliverables/new_ar_users_guide.pdf (accessed October 10, 2010).

[7] ISO (2005), Information Technology – Security Techniques – Information Security Management Systems – Requirements, ISO/IEC 27001, ISO, Geneva.

[8] Karamizadeh, S., Shayan, J., Alizadeh, M., &Kheirkhah, A. (2013). Information Security Awareness Behavior: A Conceptual Model ForCloud.International Journal Of Computers & Technology, 10(1), 1186-1191.

[9] Lee, Y., and Kozar, K. A. (2005). Investigating factors affecting the adoption of anti-spyware systems.Communications of the ACM.

[10] Peltier, T.R. (2005), "Implementing an information security awareness program", Information Systems Security, Vol. 14 No. 2, pp. 37-48.

[11] Proctor, R.W and Proctor, J.D. (2006). Handbook of Human Factors and Ergonomics 3rd ed., John Wiley and Sons, New York

[12] Puhakainen, P. (2006), "A design theory for information security awareness", doctoral dissertation, Department of Information Processing Science, University of Oulu, Oulu, available at: http://herkules.oulu.fi/isbn9514281144/ (accessed January 10, 2010).

[13] Qing, H., Hart, P. and Cooke, D. (2007), "The role of external and internal influences on information systems security a neo institutional perspective", Strategic Information System, Vol. 16 No. 2, pp. 153-72.

[14] Rhee, H. S., Kim, C., &Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & Security, 28(8), 816-826.

[15] Richardson, R. (2007). CSI Computer Crime and Security Survey. Computer Security Institute. From: retrieved November 16, 2007.

[16] Siponen, M. and Willison, R. (2007), "A critical assessment of IS security research between 1990-2004", in O ¨ sterle, H., Schelp, J. and Winter, R. (Eds), Proceedings of the Fifteenth European Conference on Information Systems, University of St Gallen, St Gallen, pp. 1551-9.

[17] Siponen, M.T. (2000), "A conceptual foundation for organizational information security awareness", Information Management & Computer Security, Vol. 8 No. 1, pp. 31-41.

[18] Spears, J. and Barki, H. (2010), "User participation in information systems security risk management", MIS Quarterly, Vol. 34 No. 3, pp. 503-22.

[19] Tsohou, A., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2008), "Investigating information security awareness: research and practice gaps", Information Security Journal: A Global Perspective, Vol. 17 Nos 5-6, pp. 207-27.

[20] Tsohou, A., Karyda, M., Kokolakis, S., &Kiountouzis, E. (2012). Analyzing trajectories of information security awareness. Information Technology & People, 25(3), 327-352.