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

The Main Factors Influencing Information Security Behavior

Hanieh Yaghoobi Bojmaeh
London Metropolitan University
London,United Kingdom

Abstract: This paper attempts to investigate the impacts of main factors influencing information security behavior in improving awareness and performance of ICT departments' staff. According to the extant research, there are four groups of factors influencing information security behavior namely self-efficacy, intention to IT security practice, security practice-care behavior, and security practice-technology. The results of analyzing 220 gathered data from five Iranian universities showed that all factors have significant and positive impact on information security behavior, and the highest impact refers to security practice-care behavior.

Keywords: Self-efficacy, Intention to IT Security Practice, Security Practice

1. INTRODUCTION

Because of managed information system security (IS), emphasize on security of IS studies go further than technical consideration and it has close relationship to organizational and individual perspective to reach key goals in system. Regarding organizational level, there is no gradual growth of the breaches for the information security and also included risks to take place which threat individuals in organizations. Moreover, achieving a better knowledge of information system security within ethical field is according to mentioning it at combination stage of organization and technology. According to (Segev et al., 1998), in order to reach security utilizing technology is not enough but rather the organization itself does matter. Besides, it should be mentioned that IS security at both organizational and technical level (Trom Peter and Eloff, 2001) as well as its implementation has to have cognizance of both human and ethical considerations.

Also the cornerstone of information system security goals which are the foundation of secure system functions in past and critical reasons of methodology developments, were integrity, confidentiality and also data availability that needs to be followed by measures of value in order to avoid any inability issues in managing the IS security. Therefore, in current project, the method of combining different organizational and social variables to make sure IS security has been considered.

The IS security will still present a problem for professionals and also executives. Most of the studies on IS security are in nature technical and have limited emphasize on organizational and individual issues. Today, unfortunately, many firms do not have enough consideration on individual value and so they just emphasize on technical facets. Because of technical failures and human errors, organizations need to be aware about necessity of educating responsible employees in order to reinforce IS security. In this article, ICT departments of many universities in Iran have been chosen as study scope. It means that this study attempts to understand the key influential elements impacting behavior of IS security in universities of Iran.

2. LITERATURE REVIEW

According to Martins and Eloff (2003), guidelines and instructions of awareness are important aspects of maintaining stability. Also each client should be trained through stability awareness with their influential role in protecting possessed details (Lee and Larsen, 2009). It utilizes an ongoing protection awareness program for training as a probable compound in defense system of enterprise property. The specific intention of this program is enhancing the attention of users about risks and also the importance of resource security methods, particular safety of tools as well as related consequences of illegal measurements.

In addition Lee and Larsen (2009) stated that firms have to emphasize on protection awareness and provide their plans as clear as possible for making sure that there is no security problem within organizations (Woon and Kankanhalli, 2007). It will suggest a chaos of customers in protection issues that casually will take the potential risks through specific natural activities. In addition Woon and Kankanhalli, (2007) asserted that a successful firm would be safe if it provides awareness programs in certain considerations. Thus, IS can be very helpful if individuals know how to use them.

The Protection Motivation Theory (PMT) that was presented by Rogers in 1983 elaborated the model of health-related belief within health and social psychology area. Based on theories of expectancy-value and also theories of cognitive processing, PMT has been developed in order to contribute to demonstrate fear appeals. PMT was assumed as one of the best and influential explanatory theories in order to predict the attention of an individual to participate in protective acts (Anderson and Agarwal, 2010). In fact, protection motivation originates from both coping and threat appraisals. The threat appraisal defines the assessment of a person of the danger level imposed by a threatening phenomenon (Woon et al. 2005). It includes the below two items:

(i) Perceived vulnerability is a personal assessment about possibility of threatening phenomenon. In this paper, threats are initiating from non-compliance with ISSP.
(ii) Perceived severity means those severities which are the results of event. Here, imminent threats

toward security of information in an organization come from non-compliance with ISSP. The aspect of coping appraisal of the PMT means the individual's evaluation of their capability to deal with and also avert the potential damage and loss originating from a threat (Woon et al., 2005). Such coping appraisals have three main sub-constituents:

(i)

Self-efficacy: this variable focuses on a person's judgment or capability about their abilities to deal with or perform the suggested behavior. In this paper, it means those types of measures and skills which are necessary for protecting the information in an IS context within an organization (Bandura, 1991; Woon et al., 2005 and Pahnila et al., 2007).

(ii)

Response efficacy: it is about those beliefs on perceived advantages of the taken action by people (Rogers, 1983). In this study it means having compliance with ISSP as an effective approach to detect any threat to organizational IS properties.

(iii)

Response cost: this element refers to the perceived opportunity costs of monetary, effort ad time in order to perform the suggested behavior, in this case means complying with ISSP.

Moreover, it was demonstrated that people's behavior in fact is impacted or influenced by what they see as typical within an environment (Chan et al., 2005; Knapp and Marshall, 2006; Johnson and Warkentin, 2010).

Moreover self-efficacy reveals the knowledge and characteristics of an individual to manage any task or maybe contribute to make many alternatives (Bandura, 1991). This concept has been demonstrated to have a remarkable impact on capabilities of a good individual to conduct a task behavior that includes usage too (Compeau and Higgins, 1995; Workman et al., 2008).

Many investigations have coped with remarkable dysfunction since self-efficacy pertinence does not have compliance with conformity behavior intention of ISSP (Bulgurcu et al. 2010; Pahnila et al., 2007; Herath and Rao, 2009a; Larose et al., 2008; Workman et al., 2008).

Previous scholars that employed PMT realized that it is helpful in forecasting the related behaviors to people's computer security behaviors in both organizations and at home (Lee and Larsen, 2009 and Anderson and Agarwal, 2010) and also compliance of ISSP (Herath and Rao, 2009; Pahnila et al., 2007).

Various researchers (e.g. Karamizadeh et al., 2013; Rhee et al., 2009; Richardson, 2007; Proctor et al., 2006; Lee and Kozar, 2005) have highlighted different factors which have high potential to affect information security behavior. These factors are self-efficacy, intention to IT practice, security practices (care behavior), and security practices (technology). It suffices that this study also applies these factors for its scope. The proposed framework of this study is demonstrated figure 1.

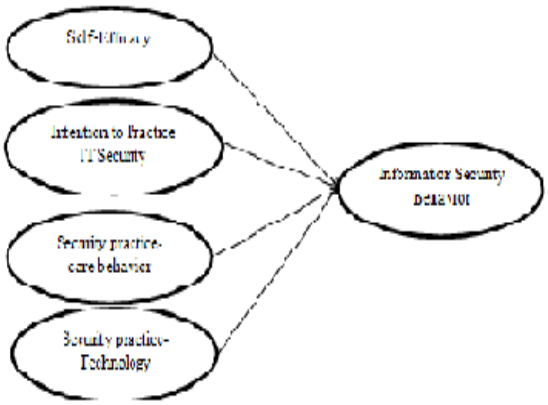

Figure1: Proposed Framework

3. METHOD AND RESULTS

This study applied quantitative approach to measure the impact of highlighted factors on information security behavior. In this regard, four hypotheses were developed as followings.

H1: Self-efficacy has a significant and positive impact on information security behavior

H2: Intention to practice has a significant and positive impact on information security behavior

H3: Security practice-care behavior has a significant and positive impact on information security behavior

H4: Security practice-technology has a significant and positive impact on information security behavior

To measure the underlying factors of this study, the questionnaire of the Karamizadeh et al. (2013) were applied. According to their research, self-efficacy consists of two dimensions namely IT knowledge and computing behavior. Intention to practice IT security is measured by IT literacy and security measures. Security practice-care behavior refers to online file-sharing and data protection, while security practice-technology refers to antivirus and spam filtering.

The population of this study was all members of staff (managers, engineers and technicians) who work in ICT departments of 5 large universities located in Tehran. The sample size was 220. The results of reliability test shows that all variables have good or excellent internal consistency. To test above hypotheses, first Pearson correlation test was applied. The results showed that each independent variable has significant relationship with information security behavior. The highest relationship refers to security practice-

care behavior, while the lowest relationship refers to the self-efficacy to practice.

Table1: Correlations

SELFEFF	Pearson Correlation	1	-.008	-.018	.001	.136*
	Sig. (2-tailed)		.912	.787	.988	.041
	N	220	220	220	220	220
INTENTION	Pearson Correlation	-.008	1	.157**	.000	.311**
	Sig. (2-tailed)	.912		.020	.994	.000
	N	220	220	220	220	220
SEC CARE	Pearson Correlation	.018	.137*	1	.189**	.553**
	Sig. (2-tailed)	.787	.043		.005	.000
	N	220	220	220	220	220
SEC TECH	Pearson Correlation	.001	.000	.189**	1	.540**
	Sig. (2-tailed)	.988	.994	.005		.000
	N	220	220	220	220	220
ISBEHA	Pearson Correlation	.136*	.311**	.553**	.540**	1
	Sig. (2-tailed)	.041	.000	.000	.000	
	N	220	220	220	220	220

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.

Table2: Coefficients from Regression Analysis

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.538	.365		1.474	.142
	SELFEFF	.167	.066	.133	2.538	.012
	INTENTION	.177	.065	.168	2.707	.007
	SEC CARE	.315	.069	.288	4.573	.000
	SEC TECH	.202	.064	.193	3.149	.002

a. Dependent Variable: ISBEHA

As shown in table 2, all of the independent variables have significant impact on information security behavior since all estimated coefficients are less than .05. Hence all of the hypotheses of this study are supported by obtained results. As summary, the outcome of regression analysis can be written as following equation:

IS Behavior =.538+.167 (Self-Eff) + .177 (Intention)+ .315 (Sec-care)+ .202 (Sec-Tech)

4. CONCLUSION AND DISCUSSION

The obtained results demonstrated that all of the highlighted factors have significant influence on information security behavior. On the other hand, ICT departments in Iranian universities can improve these factors in order to reinforce their information security behavior. Since most of the impact is on security practice-care behavior so considering the online file sharing and also data protection are very important. The future studies can test the framework of this research in other scopes. Moreover, the amount of R-Square in this study is not high thus it is possible that other factors also could be added to this framework. Besides, future researches can focus on some factors such as human resource practices and transformational leadership. Using such factors will make a bridge between human resource management and information security.

5. REFERENCES

[1] Anderson, C. L., Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *Mis Quarterly.* 34(3), 613-643.

[2] Bandura, A. (1997). toward a unifying theory of behavioral change. *Psychological review.* 84(2), 191.

[3] Bandura, A(1991). Social cognitive theory of self-regulation. *Organizational Behaviour and Human Decision Processes.* 96(3), 160.

[4] Chan, M. Woon., and Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of information privacy and security.* 1(3), 18-41.

[5] Compeau, D. R., and Higgins, C. A. (1995). Computer self-efficacy: development of a measure and initial test. MIS Quarterly.

[6] Hsu, M. H., and Chiu, C. M. (2004). Predicting electronic service continuance with a decomposed theory of planned behaviour. *Behaviour and Information Technology.* 23(5), 359-373.

[7] Herath, T., and Rao, H. R. (2009a). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems.* 18(2), 106-125.

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

[9] Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. MIS quarterly, 34(3), 549-566.

[10] Knapp, K. J., and Marshall, T. E. (2006).Information security: management's effect on culture and policy. *Information Management and Computer Security.* 14(1), 24-36.

[11] Kankanhalli, A., Tan, B. C. Y., and Wei, K. K. (2005). Contributing knowledge to electronic knowledge repositories: An empirical investigation. *Mis Quarterly*, 113-143.

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

[13] Larose, R., and Rifon ,N. J. Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM.* 51(3), 71-76.

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

[15] Lee, Y., and Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. European Journal of Information Systems.

[16] Martins, A., and Eloff, J. (2003). Information Security Culture, Proc. of IFIP TC11 17th International Conference on Information Security (SEC2002), Cairo, Egypt. IFIP Conference Proceedings.

[17] 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.

[18] Pahnila, S., Siponen, M., and Mahomood, A. (2007). Employees' behaviour towards IS security policy compliance. In: Proceedings of the 40th Hawaii International Conference on System Sciences, January 3e6, Los Alamitos, CA.

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

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

[21] Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology*, 153-176.

[22] Segev, A., Porra, J., & Roldan, M. (1998). Internet security and the case of Bank of America. Communications of the ACM, 41(10), 81-87.

[23] Trompeter, C. M., & Eloff, J. H. P. (2001). A framework for the implementation of socio-ethical controls in information security. Computers & Security, 20(5), 384-391.

[24] Torkzadeh, G., and VanDyke, T. P. (2001). *Development and validation of an internet self-efficacy scale Behaviour and Information Technology.*

[25] Woon, I., Tan, G., and Low, T. (2005). A protection motivation theory approaches to home wireless security. In: Avison D, Galletta D, DeGross JI, editors. Proceedings of the 26th International Conference on Information Systems, In Las Vegas, December P.

[26] Woon, I., and Kankanhalli, A. (2007). Investigation of IS professionals' intention to practise secure development of applications. International Journal of Human-Computer Studies.

[27] Workman, M., Bommer, H. H., and 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.