Journal of American Science

Websites:
http://www.jofamericanscience.org
http://www.sciencepub.net

Emails:
editor@sciencepub.net
sciencepub@gmail.com

MARSLAND PRESS
Multidisciplinary Academic Journal Publisher

Information security behaviours in enhancing awareness

Sasan Karamizadeh

Advanced Information School (AIS), University Technology Malaysia (UTM), Kuala Lumpur, Malaysia)
Ksasan2@live.utm.my

Abstract: The main objective of the study is to investigate the components affecting information security behaviour in enhancing awareness and design an information security behavior model in enhancing awareness. Cross sectional study is conducted among students currently studying in University Technology Malaysia. Quantitative data are collected through a self administrated questionnaire consisting of 6 sections based on previous studies. Moreover, the sample is selected among students who are pursuing bachelor, master and PhD programs in international campus of University Technology Malaysia. The study has found significant relationship between self-efficacy, security practice- care behaviour, security practice- technology on information security awareness behaviour. The study does not show significant relationship between intention to use IT practice and information security awareness behaviour. At the end, recommendations for future studies and limitations of the study were further established.

[Karamizadeh S, **Information security behaviours in enhancing awareness,** *J Am Sci* 2022;18(8):23-32]. ISSN 1545-1003 (print); ISSN 2375-7264 (online). http://www.jofamericanscience.org. 03. doi:10.7537/marsjas180822.03.

Keywords: Self Efficacy, Technology Behaviour, Care Behaviour, Intention, Information security awareness.

1. Introduction

Organisations tend to heavily depend on Information Technology (IT) for the matter of their success. It is because such systems typically guard data sources while protecting valuable informational assets. Information Technology is also used to maintain assets in systems away from misuse, mistreatment and deterioration. Organizations frequently conduct technical actions for that means. Adding firewalls, upgrading anti-virus software, system backups their systems, keeping and constraining accessibility controls, using encryption keys, and making use of comprehensive checking systems are among those actions (Woon and Low, 2005). Nevertheless, these methods and measures offer partial technical or technological means to fix the problem, and are rarely ample in supplying total protection (Krejcie and morgan, 1970). Researchers like (Pahnila and luthans, 2007)possess those businesses that pay attention to technical as well as non-technical aspects that imply guarding of Information Security (IS) assets. Such resources are likely to be more lucrative in their attempts to protect their particular key IS assets."

To strengthen the knowledge of Information Systems Security Policy (ISSP), protection motivation theory (PMT) is formulated. PMT has been used as a model for influencing and predicting different behaviour. In this study PMT has been used for predicting information security behaviours among university student. Towards the researcher's very best of knowledge, no prior researcher has used the two concepts in a single study. Review of the literature indicated that these particular two previous hypotheses have been employed by ISSP compliance research."

"The particular responsibility thus remains with companies to utilize multi-perspective methods for defending their IS assets and resources (Herath and Rao, 2009b). For illustration, in our study, the actual tradeoffs between computer security protection and convenience, figured that employees are more likely to sidestep security procedures in order to accomplish a task (Herath and Rao, 2009b). Against this kind of a foundation, it is a beneficial approach for agencies to pay attention to their employees' motives and habits as well. Lately, research has surfaced to indicate the pertinence of employees' compliance together with business rules, guidelines, and specifications outlined in their particular ISSP as a helpful procedure for shaping or influencing the behaviours of their employees regarding how firms' IS resources are widely-used (Cavusglu et.al 2004;Chan et,al;2005 ; Pahnila et.al . 2007; Buluurcu et.al. 2010; Ifinedo, 2011).

The same stream of literature additionally suggests that wherever these kinds of ISSPs are located to assist shielding versus incorrect usage, misuse, or damage of assets, employees may not tend to abide these kinds of documents (Pahnils et.al 2007; Sekarau, 2010). Therefore, the studies that are designed to increase the awareness towards information security behaviour are useful to extend the literature. Security risks related to IT are subjective and have become increasingly important because people are strongly dependent on technologies such as Internet. In other words, information security has become a key concern among people using email, online games, data file sharing and so on.

Various issues related to Information Security (IS) raised in university computer networks in early 1975. Universities and educational institutions are usually the targets for cyber attacks because of two major reasons (Knapp et. al .2006). First, simply because of the large number of computing activities; and secondly universities offer the students an open access to wide range of information. Overall it increases the potential risk of being a victim of cyber-attack. This research attempts to investigate the components affecting information security behaviour in enhancing awareness.

2. Material and Methods

2.1 Information Security Awareness (ISA)

Marint,(2003), claims that awareness instructions and guidelines are vital parts of defending stability. In addition, every client must be educated by means of stability awareness, with their effective role in protecting details that are possessed (Lee and Larson, 2009) . It employs a continuous protection awareness training program as a possible compound in the enterprise property defense system. The specific program's intention is to increase users' attention of the risk and the necessity regarding resource security techniques, particular tool safety along with the consequences associated with illegal measures.

Lee and Larsen, (2009), believe that companies should focus on protection awareness and make their own plans elaborately clear in order to ensure that there is no security issue in the organization (Woon and Low, (2005). It proposes a chaos of consumers in protection problems which casually take the potential risks by their certain natural actions. Woon and Low, (2005) state that a successful company is safe when it put awareness programmed under serious consideration. Therefore, information systems might be very useful only when people are aware of using them.

2.2. Protection motivation theory[PMT]

Protection Motivation Theory (PMT), which developed by Rogers (1983) expanded the health-related belief model in the social psychology and health domains and (Milne and Orbell, 2000). Drawing from the expectancy-value theories and the cognitive processing theories, PMT was developed to help clarify fear appeals. PMT has been noted as one of the most powerful explanatory theories for predicting an individual's intention to engage in protective actions (Anderson and Agarwal, 2010). In essence, protection motivation emanates from both the threat appraisal and the coping appraisal. Threat appraisal describes an individual's assessment of the level of danger posed by a threatening event (Woon et.al ,2005). It is composed of the following two items:

(i)

Perceived vulnerability is an individual's assessment of the probability of threatening events. In this study, threats resulting from noncompliance with ISSP.

(ii)

Perceived severity is the severity of the consequences of the event. In this instance, imminent threats to the security of one's organization's information arising from noncompliance with ISSP.

The coping appraisal aspect of PMT refers to an individual's assessment of his or her ability to cope with and avert the potential loss or damage arising from the threat (Woon et.al, 2005). Coping appraisals are made up of three sub-constituents:

(i)

Self-efficacy – this factor emphasizes the individual's ability or judgment regarding his or her capabilities to cope with or perform the recommended behavior. In the context of this research, it refers to the sorts of skills and a measure needed to protect the information in one's organizational IS (Bandura, 1991;Woon et.al , 2005; Pahnila et.al, 2007).

(ii)

Response efficacy – this factor relates to the belief about the perceived benefits of the action taken by the individual (Richardson, 2007). Here, it refers to the compliance with ISSP as being an effective mechanism for detecting a threat to one's organizational IS assets.

(iii)

Response cost – this factor emphasizes the perceived opportunity costs in terms of monetary, time, effort expended in adopting the recommended behavior, in this instance complying ISSP.

Furthermore, It's been revealed that individual's behaviour is actually influenced or inspired by what they view to become typical in environment (Chan et.al, 2005; Jonhston and Warkentin, 2010; Knapp and Marshall, 2006).

Self-efficacy highlights the individual's features and knowledge to manage the task or perhaps help to make an alternative [4]. Self-efficacy has been shown to have got a significant impact on a good individual's capability to accomplish task behaviour, which includes usage (Comteau and Higgins, 1995; Workman et.al ,2008).

Numerous studies have encountered significant dysfunction due to the fact that the pertinence of self-efficacy do not comply with the ISSP conformity behaviour intention (Bulgurcu et.al. 2010; Pahnila et.al, 2007; Heeath and Rao , 2009b; Larson et.al ,2008; workman et.al ,2008).

Previous researches that have used PMT found it useful in predicting behaviours related to individual's computer security behaviours both at home and in organizations (Anderson and Agarwal, 2010; Leee and Larsen, 2009), and ISSP compliance (Pahnila et.al ,2007; Herath and Rao, 2009b).

2.3 Self-Efficacy

Self-efficacy is a key element in the formation of social cognitive theory. It's a form of self-evaluation that is a proximal determinant of individual's behaviour (Bandura, 1997). People with a high level of self-efficacy have got stronger form of conviction regarding their capability to mobilise motivation, cognitive resources and course of action needed to efficiently implement a task. Self-efficacy affects directly or indirectly on amount of effort, self-regulations, and the initiation and persistence of coping efforts in facing obstacles (Bandura, 1997). The empirical validity of this argument has been documented in a variety of research contexts (Bandura, 1997) .

Self-efficacy researchers highlight that, in order to enhance the predictability of self-efficacy in performance, the domain specificity of SE should be considered. Bandura, (1997) cautions against the use of context less measures of SE. Consistent with this domain-specific argument, Marakas, (2007)explain the concept of computer self-efficacy by considering both the general and task specific levels.

Moreover, social cognitive theory also focuses on the role of self-efficacy on behaviour control over potentially threatening events. In other words, people with a strong sense of self-efficacy are likely to pay their attention on analyzing and formulating solutions to problems.

Regarding to the study of (Hyeun et.al, 2009), individuals with more experience in computer or internet use will have higher levels of self-efficacy on tasks that require protecting their information and information systems.

Additionally, internet self efficacy has turned out to be a beneficial impacting factor for internet consumption (Larson et.al, 2008) and the employment of e-service (Hsu and Chiu , 2004). In a current work by (Whitten , 2004). self-efficacy has been discovered to get a significant part of forecasts regarding security functions in cell phone sites.

Hypothesis 1: there is a positive significant relationship between self efficacy and ISA behaviour.

2.4. Security Practice Behaviour

According to social psychological theory on information security platform, when individuals start to believe in protection of their own information and information systems, they tend to help in the process of improving security methods and show positive intentions to the organization to continue its efforts on the current system.

A computer security incident is defined as a security-related adverse event in which there is a loss of information confidentiality, disruption of information or system integrity, disruption or denial of system availability, or violation of any computer security policies. According to the 2007 annual survey conducted by the Computer Security Institute (Rhodes, 2001), 46% of respondents indicated that their organization experienced a security incident within the last 12 months. Of these, a significant number (52%) of the attacks are virus-related. It is consequently important for organizations and employees to be aware of and protect themselves against security threats and cybercrime.

While many consultant guidelines are available, there is a lack of empirical studies concerning the design and effectiveness of security awareness programs. On the other hand, many studies have been conducted to investigate how to encourage people to follow information security practices from different angles. Whitten presented an analysis of information security from the perspective of usability and developed design principles for usable security (Lee and Larson, 2009). Schultz and his colleagues proposed taxonomy of usability for security controls and explained why each element of the taxonomy was necessary(Stanton et.al, 2005). The two factors of taxonomy are illustrated in Figure 1.

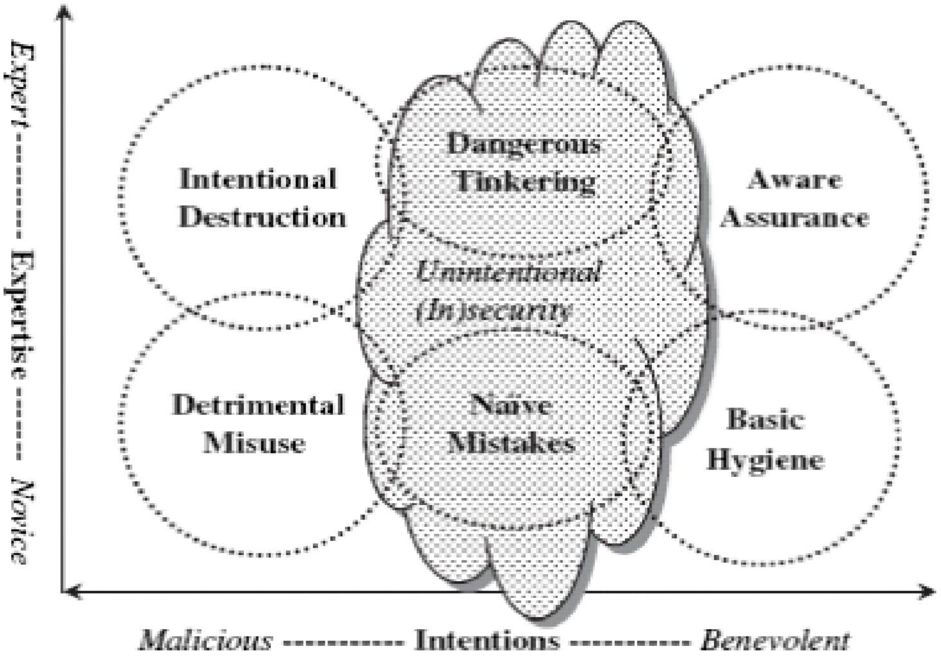
Expert ---------- Expertise ---------- Novice
Intentional Destruction
Dangerous Tinkering
Aware Assurance
Unintentional (In)security
Detrimental Misuse
Naive Mistakes
Basic Hygiene
Malicious ----------- Intentions ----------- Benevolent

Figure 1: Two-factor Taxonomy of End-user Security Behaviours
Source: (Stanton et.al, 2005).

Adams and his colleagues looked at user interface issues related to passwords. They found that fear was a useful mechanism for getting people to follow password policies (Adams et.al 1997). If users fear the consequences and impact of security threats, or if users think the security threats are severe, they will be more likely to follow the security procedures. Proctor et.al (2006), presented a case study of applying human factors analysis in information security and claimed that human factors analysis can reveal reasons for users' acceptance or rejection of particular security controls and procedures.

Moreover, various dimensions of security practice behaviour are necessary for a better effective risk management. Training security awareness care-behaviour together with entitlement of security software decreases some weakness of information security and increases the use of security software on its own. The impact of computer self efficacy concerning computer usage and ownership is shown in earlier reports. Research about CSE has proved that it is not easy to be optimistic in the relationship between users' confidence in his or her computing skills and utilization of information systems .

People together with a powerful awareness of self-efficacy are usually concentrating their consideration in analyzing and making answers to issues of information security (Bandura, 1991). Those with decreased self-efficacy have got a propensity to have interaction in much less management problem efforts.

It benefits those who practice recommended security awareness behaviours to protect their information and information systems. Therefore, the following hypothesis is proposed based on the literature:

Hypothesis 2: there is a positive significant relationship between security practice- care behaviour and ISA Behaviour.

2.5. Security Practice- Technology

The particular growing set of information security dangers and the actual ever-growing body of rules has made information security an essential function within many areas of businesses. However, many companies find it difficult to access sources that protect hazards imposed on their information security. Securing networks can be done through implementing a mix of anti-virus or anti-spyware software, firewalls, intrusion prognosis and reduction systems, and articles filtering software. Nevertheless, this specialized layer of defence to an organization's security may falter to human disappointment (Hus and Chiu, 2004).

Organizations are actually facing problems in their securities with all the introduction of electronic commerce and open up network architectures. Much better computer reading and writing, improved computer literate personnel and accessibility to superior software methods might also contribute to the increase in security violations in future. And therefore, management must pay more attention to potential security problems (Peterson and Luthans, 2006) .

There are several credible explanations for minimal management concerns about security (Kankanhalli et.al, 2005) : (a) managers can make strategic decisions leading to lesser security as they generally consider the actual risk of security violations, (b) managers may be sceptical in regards to information security success due to difficulty in assessing its benefits, and (c) managers may possibly lack knowledge regarding the array of controls available to decrease IS abuses. In order to raise managements' interest to be constantly involved with security selections, it is very important to inform and impress them with the benefits of IS; Introduce them security initiatives and educate them on the proper kind of IS that is appropriate to their own organization. It is essential to convince them for taking those security steps that are effective and inexpensive subjective to their own structures (Kankanhalli et.al, 2005).

Information security awareness is a powerful process and it becomes more vital in environments in which risks continually change. Accordingly, any awareness program needs to be constantly assessed and managed to keep an update of alterations in risk profiles. To maintain a person's current and future mindset restored, any kind of awareness program has to be continuous and at the end to be an integral part of the organization culture. The key to achieving the best results in awareness is through maintaining the message particularly customized to different employees, having it constant while differentiating its delivery method, to hold everybody fascinated (Whitman and Mattord, (2003).

The general statistics indicate that most of the virus activations are from users' unintentional downloads from e-mails or a web sites accompanied with their lack of knowledge (Whitman and Mattord, (2003). Even though use of a strong anti-spyware program may effectively protect systems attacks, the actual rate of using these soft wares by customers is as little as 10 percent (Lee and Kozar, (2005). reports that more than fifty percent of almost all security breaches are due to social engineering and users' sloppy behaviour. According to results of these scientific studies, security practice – technology positively influences individuals' behaviour. Therefore, the following hypothesis is proposed based on the literature:

Hypothesis 3: there is a positive significant relationship between security practice- technology and ISA Behaviour.

2.6. Intention to practice IT security

In today's highly interconnected world, cyber security is a serious issue that requires attention. With 888 million Internet users (Internet Usage Statistics 2005), it is imperative to study the security of home computers connected to the Internet, as it has a direct impact not just on individual computers, but the security of the cyberspace, including critical infrastructures and services (such as telecommunication and banking) that are heavily dependent on the secure functioning of the cyberspace. Undefended home computers can become part of networks of remotely controlled machines that are then used to attack critical infrastructures. Thus, we consider the practice of home computer security as a socially and personally positive behaviour as it protects one's home computer and contributes to the security of the cyberspace.

Information systems (IS) cannot be effective unless they are used. However, people sometimes do not use systems that could potentially increase their performance (MAthieson, 1991). Behavioural intention measures individuals' willingness to continue their efforts in order to strengthen their security measures (Hyeun et.al, 2009).

One of the biggest threats to home computer security is virus infection, which has the potential to threaten the confidentiality and integrity of information on computers as well as the availability of computers and networks. The damage is not limited to just home users, as the security of the cyberspace is affected (Bandura, 1997).

Therefore, the behaviour of home computer users on computer security issues is probably one of the most important factors in determining whether these systems are sufficiently secured. Unfortunately, home computer users are generally unprepared to defend against attacks from the Internet (Carpenter, et.al , 2001).

In summary, based on the findings and discussions in other studies related to intention to use IT practice, the following hypothesis is proposed:

Hypothesis 4: there is a positive significant relationship between intention to use IT practice and ISA Behaviour.

Figure 1 shows the conceptual model of the study. As it is shown, there are four independent variables which are; self efficacy, security practice- care behaviour, security practice- technology, intention to practice IT securities. Furthermore, the dependent variable is information security awareness behaviour.

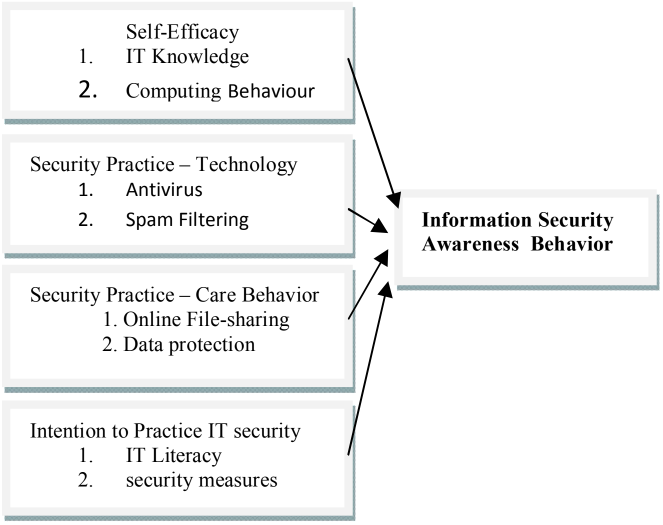

Figure 1: Proposed Model of Information Security Awareness Behaviour

3. Results

After gathering 180 data from university's students, reliability test showed all variables have good or acceptable internal consistency (based on Nunally's argument in 1978) because all value were more than 0.7.

A correlations test was conducted to determine the correlation between independent variables and the dependent variable which is information security awareness behaviour. The correlation has been clearly exhibited in the Table 3.1.

Table 3.1: Pearson's Correlations

		Self-Efficacy	IT security care behaviour	Intention to practice IT security	ISA	Security practice-Technology
Self –Efficacy	Pearson Correlation	1				
	Sig.(2-tailed)					
IT security care behaviour	Pearson Correlation	-.038	1			
	Sig.(2-tailed)	.706				
Intention to practice IT security	Pearson Correlation	.038	.088	1		
	Sig.(2-tailed)	.709	.385			
ISA	Pearson Correlation	.559	.210	.040	1	
	Sig.(2-tailed)	000	.036	.690		
Security practice-Technology	Pearson Correlation	-.048	.130	-.016	.325	1
	Sig.(2-tailed)	.636	.196	.873	.001	

Variables	H	β	Std. Error	t-value	p-value	VIF
Constant		-0.469	.446	-1.051	296	
Self -Efficacy	H1	0.376	.086	4.357	.000	1.020
Security Practice-Technology	H2	0.572	.073	7.789	.000	1.005
Security Practice- Care Behaviour	H3	0.0181	.072	2.498	.014	1.025
Intention to PracticeIt Security	H4	0.007	.072	.925	.925	1.010

Based on the Table 4.1, self efficacy has the strongest association with the variable ISA with a value of 0.559 in 0.01 significance level. Moreover, there is correlation between IT security care behaviour and ISA at 0.05 significance level. It means when IT security-care behaviour increases, information security awareness increases as well. Furthermore, correlation is found between security practice-technology and information security awareness at 0.01 significance level. In other words, by increasing security practice-technology, information security awareness will increase. In following, multiple regression analysis shows the significance of each independent variable on dependent variables. (See Table 2)

Multicolinearity is contributed to the highest correlation between independent variables. Saunders et.al, (2007) Discussed VIF value which is higher than 10, determine great independency between IVS. Based on this issue, as Table 4.12 shows all VIFs are below 10. Therefore it cannot have a significant multicolinearity relationship among independent variables.

Furthermore, R square shows the percentage of variance in the dependent variable that is explained by the variation in the independent variable (Sekaran, 2010). R square is 0.472 which shows that 47.2% of variation in the dependent variables can be explained by the independent variables.

As a summary, due to the result of regression analysis three hypotheses are supported in this study and one of them is not. The equation model is drawn in following:

ISA= -0.0469 + 0.572(Technology) + 0.376 (Self Efficacy) + 0.181 (IT security care)

4. Discussions

Organisations tend to heavily depend on Information Technology (IT) for the matter of their success. It is because such systems typically guard data sources while protecting valuable informational assets. Information Technology is also used to maintain assets in systems away from misuse, mistreatment and deterioration. Organizations frequently conduct technical actions for that means. Adding firewalls, upgrading anti-virus software, system backups their systems, keeping and constraining accessibility controls, using encryption keys, and making use of comprehensive checking systems are among those actions (Workman et. al, 2005; Lee and Larsen, 2009). Nevertheless, these methods and measures offer partial technical or technological means to fix the problem, and are rarely ample in supplying total protection (Rhodes, 2001).

Generally, 180 respondents have participated in the study. 48% were male and 52% were female that determine the lack of bias at the time of survey distribution among respondents. It was perfect to figure out that a majority of respondents are master students which show a proper qualification for this study. Overall 10 items were examined for the first variable named as self-efficacy. The mean value for the item number one was 4.58 which is the highest value compared to other items. The item focuses on knowledge and personality of the respondent more.

The proposed conceptual frameworks of the study contain four components as the independent variables which are: self-efficacy, security practice-technology, security practice care behaviour and intention to practice IT security. The study strived to find the impact of these four variables on information security awareness.

All components evaluated by survey and the results indicated that the three factors named self-efficacy, security practice technology and security practice care behaviour have impacted on information security awareness. In contrast, the component named intention to practice IT security showed the relatively low impact on information security awareness.

4.1. Limitation of the Study

This study faced with one huge limitation particularly in the first step was tendancy of respondents to fill up questionnaires. Furthermore, another limitation of the study is time limitation for distributing questionnaires.

4.2. Recommendation for Future Studies

This study has been conducted on students, it is recommended to replicate the study on staff working in public or non-public companies. Also it is a good idea to replicate the study in other countries to determine the behaviour differences in different countries. It is also recommended to extend the study into other parts of Malaysia. In other words, another study can be conducted on students studying in other universities locating in other states of Malaysia. Then, it is possible to determine the differences in information security behaviours among students studying in giant cities and small cities.

References

[1]. Adams, A., Sasse, M.A., and Lunt, P. Making passwords secure and usable. People and Computers, 1997;1-20.

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

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

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

[5]. Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly.2010;84(4), 415-643.

[6]. Cavusoglu, H., Mishra, B., and Raghunathan S. (2004). A model for evaluating IT security investments. Communications of the ACM.2004; 47(7), 87-92.

[7]. Carpenter, J., et al.Continuing Threats to Home Users. CERT Advisory CA. 2001;-2001-20

[8]. 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. 2005; 1(3), 18-41.

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

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

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

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

[13]. Hyeun, S., Cheongtag, K., and Young, U. Self-efficacy in information security: Its influence on end users' information security practice behavior. computers and security. 2009;28(8), 816-826.

[14]. Ifinedo, P. An exploratory study of the relationships between selected contextual factors and information security concerns in global financial services institutions. Journal of Information Security and Privacy;2011.

[15]. Jonhston, A. C., and Warkentin, M. Fear appeals and information security behaviors: an empirical study. Mis Quarterly. 2010; 34(3), 549-566.

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

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

[18]. Lee, Y., and Kozar, K. A. Investigating factors affecting the adoption of anti-spyware systems. Communications of the ACM Pielou EC. Ecological Diversity. Wiley, New York, 2005; 1975;165.

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

[20]. Mathieson, K. Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior. Information Systems Research. 1991; 2(3), 173-191.

[21]. Marakas, G., Johnson, R., and Paul F. The Evolving Nature of the Computer Self-Efficacy Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability Over Time., Journal of the Association for Information Systems;2007.

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

[23]. Milne, S., Sheeran., and P. Orbell, S. Prediction and intervention in health-related behaviour: a meta-analytic of protection motivation theory. Journal of Applied Social Psychology;2000.

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

[25]. Peterson , S. J., and Luthans, F The impact of financial and nonfinancial incentives on business-unit outcomes over time. Journal of applied Psychology.2006; 91(1), 156.

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

[27]. Kankanhalli, A., Tan, B. C. Y., & Wei, K. K. (2005). Contributing knowledge to electronic knowledge repositories: An empirical investigation. Mis Quarterly; 2005, 29(1), 113-143.

[28]. Krejcie, R. V., and Morgan, D. W. Determining sample size for research activities. Educ Psychol Meas; 1970.

[29]. Rhodes, K. Operations security awareness: the mind has no firewall. Computer Security Journal;2001.

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

[31]. Saunders, M., Lewis, P., and Thornhill, A. Research Methods for Business Students 3rd edition Harlow: Prentice Hall;2007.

[32]. Sekaran, U. (2010). Research methods for business: A skill building approach. Wiley-India;2010.

[33]. Stanton, J.M., Stam, K.R., Mastrangelo,. Jolton, J. Analysis of end usersecurity behaviours. Computers & Security, Vol. 24, 2005, pp 124-133.

[34]. Tan, P.Business excellence in entrepreneurship through motivation audit. Managerial Auditing Journal; 2000.

[35]. Whitten, A. Making Security Usable. Ph.D. Thesis. Unpublished PhD dissertation, Carnegie Mellon University; 2004.

[36]. Whitman, M.E. and Mattord, H.J. Principles of Information Security. Canada. Course Technology, 25 Thomson Place, Boston, Massachusetts; 2003.

[37]. Woon, I., Tan, G., and Low, T. 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;2005.

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

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

2/19/2022