An Empirical Investigation of Information System User Security- A Knowing Doing Gap Model

Khaled Abdussalam A Elkoni[1] Mohamed Abdulla Ahmed Emeigel[1] Bilal Mohammed Eneizan[2]
1.Facuty of informtics and computer, Singidumum Universty, Belgrade, Serbia
2.Department of Marketing, Jadara University, Jordan

Abstract

The research aims to develop a structural model of user knowing –doing gap and examine the information security awareness through the model and evaluate the information security awareness at industrial level. The sample of the study is 360. The study empirically tested the two small parts of the theory of planned behavior and named them model 1 and 2. The relationship of the variables were found out using the regression model. The research had total five hypothesis and all of them were supported and the results were significant. Hence concluding that (Narcissism, Vulnerability and Severity) have significant impact on Attitude while locus of control and self-efficacy have significant impact over Behavioral control.

Introduction

The human factor is one of the important components of security management and to understand the human factor and the human perception regarding information security and complying, may impact the potential preventive actions and decrease the security related concerns. According to Schultz (2004) it is difficult to measure the effectiveness of employees training regarding information security and most of the organizations assess ROI of implemented security awareness training.

The security awareness program of employees is a way to improve the users' perceptions regarding information systems. Calluzzo and Cante (2004) found the consistent results as they were expected, the most unethical issues were identified correctly by the students while conducting a study regarding the confusion college students have in discriminating between ethical and unethical attitude using information systems. However, still there were issues regarding identification of abuse the information even if there has been proper policies regarding the information security.

The users are influenced by the causes which arise risky behavior through manipulating and misusing fear, trust, the desire to be helpful (Workman, 2007). There is the influence of organization culture regarding the information security on end user behavior; such culture is implemented by top management by establishing the tendency for information security practices. According to Williams (2008) knowledge is one of the antecedents along with personal ethics and acceptable behavior that influence the behavior of end users towards following set policies and practices. Behavioral intention may be affected by the individual attitudes however there may not be the situation that the way we want to behave is different from we actually behave. There may be employees in an organization with narcissistic traits, are often found to be office bully, harmful manager, or egotistical. This probably is risky to the organization's information security. Such personality traits may be the cause for individual in engaging in risky behavior i.e. repudiation, rationalization, negligence, and sense of being privileged. Narcissism personality behavior is not limited to individuals only it can also be applied at the corporate level (Brown, 1997). Enron and General services administration are the examples of organizational narcissism. There is a concern about users who fail to follow the organization security a policy though they are aware of polices. The behavior of users who fail to follow the security policies is called omissive behavior in other words knowing–doing gap. This knowing-doing gap can be a dangerous to the information security of the organization. There may be a dangerous impact of omissive behavior on the confidentiality and reliability of the information (Williams, 2001).

The research aims to develop a structural model of user knowing –doing gap and examine the information security awareness through the model and evaluate the information security awareness at industrial level. Furthermore the proposed framework is built on the theory of planned behavior and is supported by the previous studies. This study has a special focus over intentional ignorance of security policies for the factors i.e. convenience, disrespecting the policies or lack of awareness.

Theory of planned behavior

The purpose of this theory is to predict the deliberative and planned behavior. This theory consists of an additional construct with the name of behavioral control. This variables takes into account the common situation in which persons have not a voluntary control on their behavior for example when an individual lacks any skill or resource performing a particular job (Armitage & Christian 2003). When we summarize the TPB, we simply state that there are three domains where behavioral intention is a function of any individual beliefs which include (i) behavioral beliefs which means the beliefs for the possible outcome of an indidvual behavior, (ii) normative beliefs which means the individual beliefs regarding the normative expectations of others and (iii) control beliefs which means the individual beliefs about absence or presence of factors which may support or hinder the performance of the behavior (Ajzen, 1991)

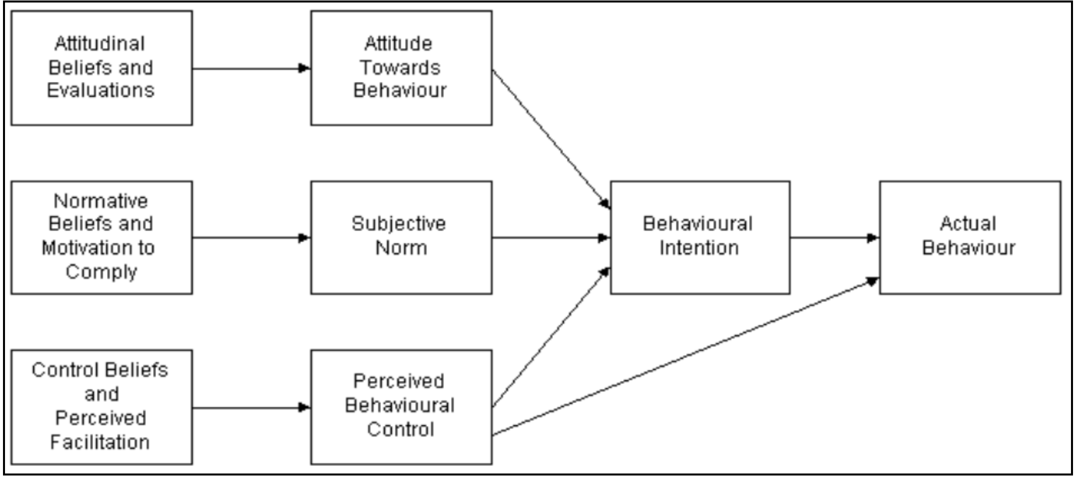

Attitudinal Beliefs and Evaluations
Attitude Towards Behaviour
Normative Beliefs and Motivation to Comply
Subjective Norm
Behavioural Intention
Actual Behaviour
Control Beliefs and Perceived Facilitation
Perceived Behavioural Control

Figure 2: The Theory of Planned Behaviour (TPB) (Source: Ajzen (1991)).

According to Armitage & Connor (2001), there are three predecessors of TPB model which are considered to be the influences on different types of behavior via the means of swaying behavioral intentions, and a large number of reviews and meta analyses summarize that TPB is a very useful theory.

From the time the TPB is introduced, numerous authors have adopted this theory as predictor to explain the behavioral intention of individuals and self reported behavior from both users and organizational perspective (Brown & Venkatesh, 2005; Chau and Hu 2002, , Pedersen 2005, Venkatesh et al. 2003). In one the study conducted by Liaw (2004) in which the model is applied to understand the behavioral intention of individuals who use serarch engine as a learning tool. Thi model is getting being largly used in technology research such as one of the study counducted by Goby (2006) who researched on online buying used the TPB model, another study used a decomposed version of this model to study electronic service continuation (Hsu & Chiu, 2004). To predict online shopping behavir, this model is also used (Hsu et al., 2006). There are few studies which have used the modified version of this model for their particular context for example, adoption of broadband internetn (Oh, Ahn and Kim 2003)) social influences in online environment (Bagozzi et al. 2006).

Threat control model

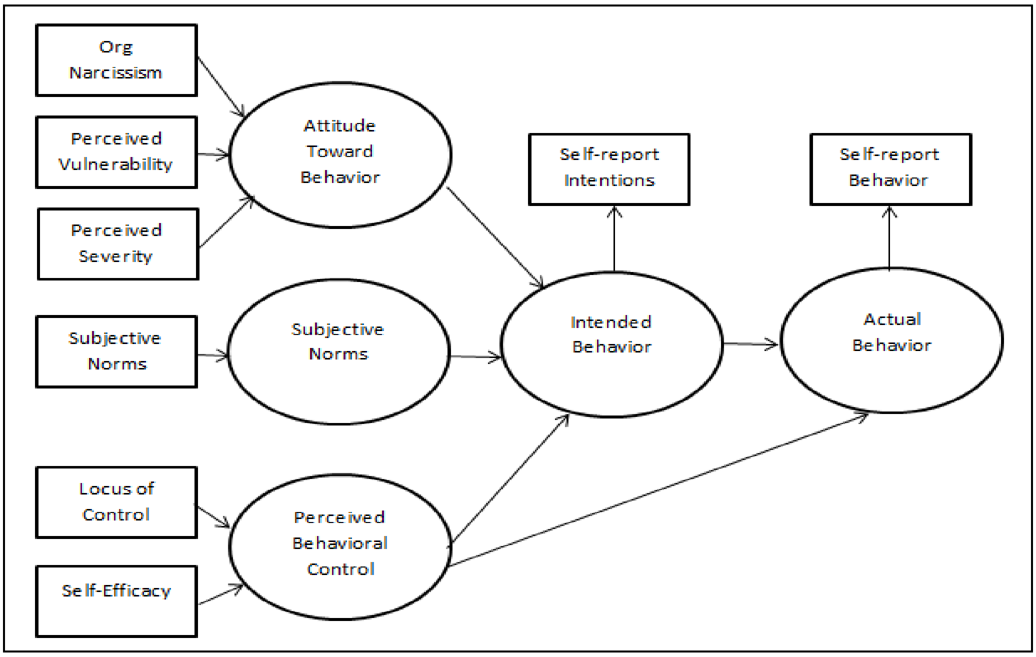
A model of omissive behavior proposed by Workman, Bommer & Straub, (2008) has two variables, namely, perceived threat and perceived coping explaining the intention of users to follow the policies of security. The model is based on some previous work using protection – motivation theory as a framework. This model is adopted to examine user omissive behavior in information security context. The threat control model is defined as an individual's threat to their self-efficacy and information are two factors which are drivers of intention to either follow or not follow the polices of security. The other construct namely coping construct is considered as the user's self-perceived abilities and desire for handling any security issues.

There are two sub variables of perceived threat namely perceived severity and perceived vulnerability. They are used separately in studies such as health belief models and protection-motivation theory (Rosenstock, Strecher, & Becker, 1988). In this context the variable perceived threat is related to the definition of risk in information security context. The risk and perceived threat is commonly used as an interchangeable term. It has also been evident in few studies (Randall & Gibson, 1991; Dinev & Hu, 2007) that user awareness of threat in IT environment is considered to be a very important predictor of attitude regarding intended behavior.

Organizational Narcissism

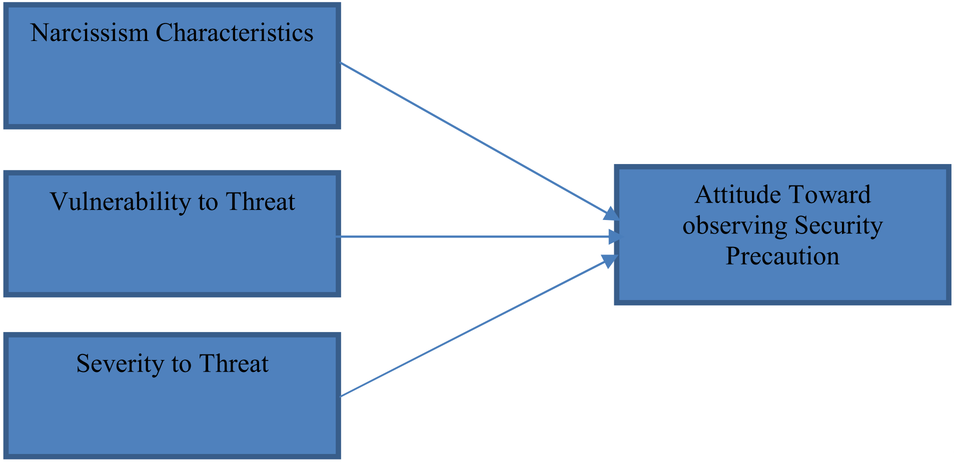
There are many perspectives form which we can find the impact of narcissists on organization security. It can be a person who is unwise risk taker and assumes that there are no rules and regulation which apply to him/her. Narcissists are imprudent which cause of self-defeating behavior for example not abiding by or following the rules (Vazire & Funder, 2006). They consider that they are permitted to work as they feel comfortable without regarding to social outcomes which may come out of their deeds (Morf & Rhodewalt, 2001). They feel they are invincible which is also a cause of their risk taking behavior (Aalsma, Lapsley, & Flannery, 2006). It is also observed that their decision making process is also more towards risk taking comparing to other people. They gamble more often with high risk relative ton non-narcissits (Lakay, Rose , Campbell and Goodie, 2008). Foster, Shenesey and Goff (2009) state that they take more risk since they believe that it may give more benefits than non-narcissists. They are considered to be over confident which modifies their ability to make sound decisions (Campbell, Goodie, & Foster, 2004). They take unnecessary risks because of their self-egos which results in avoid to follow the security policies.

Theoretical Framework

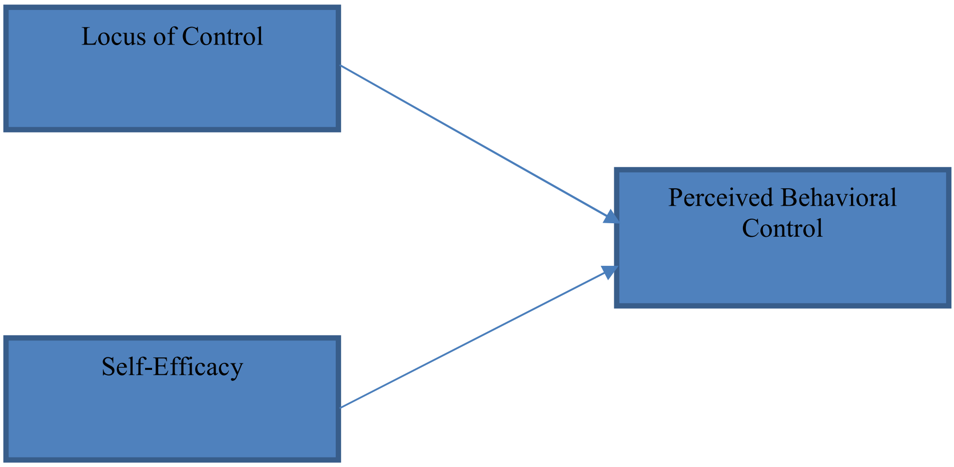


Source: Cox, J. (2012). Information systems user security

Based on the above model, the present study only focuses on two part of the study shown in the following conceptual models:


Narcissism Characteristics
Vulnerability to Threat
Severity to Threat
Attitude Toward observing Security Precaution

Conceptual Model 1



Conceptual Model 2

Hypothesis Development

The following hypothesis (1 to 3) are depicting model1 while hypothesis (4 and 5 represent model2)

H1: Users who assume narcissistic characteristics of the organization have a less positive attitude towards observing security precautions in Libyan Firms

H2: Users who perceive a higher vulnerability to the threat to their information systems have a more positive attitude towards observing security precautions in Libyan Firms

H3: Users who perceive a higher severity of the threat to their information systems have a more positive attitude towards observing security precautions in Libyan Firms

H4: Users who perceive a greater locus of control have a greater perceived behavioral control in Libyan Firms

H5: Users who perceive a greater self-efficacy have a greater perceived behavioral control in Libyan Firms

Research Methodology

The given research problem was identified from the existing literature. The conceptual frame work was validated through pilot test and expert opinion. Then data was collected from the target population through a survey instrument and was analyzed using statistical techniques including descriptive and inferential techniques such as percentage, mean, standard deviation, correlation and regression model

The population of the study is employees working in firms existing in Libya. The list of the firm was accessed. Probability sampling was used to collect the data. Under the probability sampling the random sampling method was used to draw the sample for the proposed research. The research division of the National Education Association (1960) has provided a formula for determining sample size. Based on the given formula Krejcie, & Morgan (1970) came up with a table for determining sample size for a given population for easy reference. According to the table the maximum sample size is 384. Further Barrett (2007) and Kline (2010) suggest that researcher originating from a sample size less than 200 have always been rejected. Jackson (2003). However the current research had the sample size of 360.

To collect the data from the respondent a structured questionnaire was used. The questionnaire was developed in two parts. The first part contained demographic variables while the second part was containing the questions regarding collaborative work environment, employee well-being and employee performance etc.

The questionnaires was sent to the selected organizations through email. To get the high response rate the potential respondents was reminded so as to complete the questionnaire and send it back. The ethical consideration was done before collecting the data. As the questionnaire clearly mentioned that the identity of the employees will never be disclosed. The identity of the companies will never be disclosed publicly. Furthermore, it was explicitly mentioned on the top of the questionnaire that respondents are free to quit will filling the questionnaire at any time during filling the questionnaire, even after filling the questionnaire the was asked again to use their response as the part of the research data. The permission of data collection will also be taken from the relevant authorities if needed.

Result and Findings

Reliability Analysis

Construct	Cronbach's Alpha	No of Items
Narcissism	.789	4
Vulnerability	.776	4
Severity	.701	5
Attitude	.832	4
Locus	.751	5
Self-Efficacy	.841	4
Behavioral Control	.771	4

The above table of the reliability analysis shows the scale reliability of the construct and all the constructs have the reliability statistics of the Cronbach's Alplha greater that 0.7 which means all the construct are reliable with the given number of items.

Regression Analysis Model 1

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.744[a]	.553	.549	.56461

a. Predictors: (Constant), Narcissism, Vulnerability, Severity

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	.383	.159		2.412	.016
	Narcissism	.138	.049	.119	2.809	.005
	Vulnerability	.299	.057	.310	5.273	.000
	Severity	.423	.059	.411	7.183	.000

a. Dependent Variable: Attitude

The regression model 1 shows the positive and significant impact of all the independent variables (Narcissism, Vulnerability and Severity) on the dependent variable Attitude with the t values > 2 and the p-values < 0.05, hence rejecting the null hypothesis no 1 to 3.

Regression Analysis Model 2

l Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.614[a]	.378	.374	.66525

a. Predictors: (Constant), Locus, Self-Efficacy

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	T	Sig.
1	(Constant)	.892	.182		4.897	.000
	Locus	.373	.053	.322	7.109	.000
	Self-Efficacy	.438	.046	.435	9.605	.000

a. Dependent Variable: Behavioral_Control

The above regression model 2 show that Behavioral control is affected by the locus of control and self-efficacy as the t values of both independent variables is greater than 2 and the p-value is less than 0.05 hence rejecting the null hypothesis no. 4 and 5.

Hypothesis Testing Results

Hypotheses	P-Value	Result
Hypothesis 1	.005	Supported
Hypothesis 2	.000	Supported
Hypothesis 3	.000	Supported
Hypothesis 4	.000	Supported
Hypothesis 5	.000	Supported

Conclusion

The research aims to develop a structural model of user knowing –doing gap and examine the information security awareness through the model and evaluate the information security awareness at industrial level. Furthermore the proposed framework is built on the theory of planned behavior and is supported by the previous studies. The regression model 1 shows the positive and significant impact of all the independent variables (Narcissism, Vulnerability and Severity) on the dependent variable Attitude with the t values > 2 and the p-values < 0.05, hence rejecting the null hypothesis no 1 to 3. The above regression model 2 show that Behavioral control is affected by the locus of control and self-efficacy as the t values of both independent variables is greater than 2 and the p-value is less than 0.05 hence rejecting the null hypothesis no. 4 and 5.

References

Ajzen, I. (1991), "The theory of planned behavior", *Organizational Behavior and Human Decision Processes,* vol. 50, no. 2, pp. 179-211

Armitage, C. J. & Christian, J. (2003), "Special issue: On the theory of planned behaviour", *Current Psychology,*vol. 22, no. 3, pp. 187-280

Armitage, C. J. & Connor, M. (2001), "Efficacy of the theory of planned behavior: A meta-analytic review", *British Journal of Social Psychology,* vol. 40, no. pp. 471-499.

Bagozzi, R. P., Dholakia, U. M. & Mookerjee, A. (2006), "Individual and group bases of social influence in online environments", *Media Psychology,* vol. 8, no. pp. 95-126.

Bobbitt, L. M. & Dabholkar, P. A. (2001), "Integrating attitudinal theories to understand and predict use oftechnology-based self-service: The internet as an illustration", *International Journal of Service IndustryManagement,* vol. 12, no. 5, pp. 423-450.

Brown, A. D. (1997). Narcissism, identity, and legitimacy. Academy of Management Review, 22, 643–686.

Brown, S. A. & Venkatesh, V. (2005), "Model of adoption of technology in households: A baseline model test and extension incorporating household life cycle", *MIS Quarterly,* vol. 29, no. 3, pp. 399-426.

Calluzzo, V. J., & Cante, C. J. (2004). Ethics in information technology and software use. Journal of Business Ethics, 51, 301–312.

Davis, F. D., Bagozzi, R. & Warshaw, P. R. (1989), "User acceptance of computer technology: a comparison of two theoretical models", *Management Science,* vol. 35, no. 8, pp. 982–1003.

Fishbein, M. & Ajzen, I. (1975), *Belief, attitude, intention and behavior: An introduction to theory and research,* Addison-Wesley, Reading, MA

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). *Multivariate data analysis* (Vol. 6). Upper Saddle River, NJ: Pearson Prentice Hall

Hsu, M. H. & Chiu, C. M. (2004), "Predicting electronic service continuance with a decomposed theory of planned behaviour", *Behaviour and Information Technology,* vol. 23, no. 5, pp. 359-373.

Hsu, M. H., Yen, C. H., Chiu, C. M. & Chang, C. M. (2006), "A longitudinal investigation of continued online shopping behavior: An extension of the theory of planned behavior", *International Journal of HumanComputer Studies,* vol. 64, no. 9, pp. 889-904.

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educpsychol meas*

Liaw, S. (2004), "The theory of planned behaviour applied to search engines as a learning tool", *Journal of Computer Assisted Learning,* vol. 20, no. pp. 283-291

Oh, S., Ahn, J. & Kim, B. (2003), "Adoption of broadband Internet in Korea: The role of experience in building attitudes", *Journal of Information Technology,* vol. 18, no. 4, pp. 267-280.

Pedersen, P. E. (2005), "Adoption of mobile internet services: an exploratory study of mobile commerce early adopters", *Journal of Organizational Computing and Electronic Commerce,* vol. 15, no. 3, pp. 203-221.

Schultz, E. (2004). Security training and awareness – fitting a square peg in a round hole. Computers & Security, 23, 1–2.

Sheppard, B. H., Hartwick, J. & Warshaw, P. R. (1998), "The Theory of Reasoned Action: A meta analysis of past research with recommendations for modifications in future research", *Journal of Consumer Research,* vol. 15, no. 3, pp. 325-343

Siponen, M., Mahmood, M. A., & Pahnila, S. (2009). Are employees putting your company at risk by not following information security policies? Communications of the ACM, 52, 145–147. http://dx.doi.org/10.1145/1610252.1610289.

Small-Sample Techniques. The NEA Research Bulletin, Vol. 38 (December, 1960), p. 99.

Taylor, S. & Todd, P. (1995), "Assessing IT usage: The role of prior experience", *MIS Quarterly,* vol. 19, no. 4, pp. 561-570

Venkatesh, V. & Davis, F. D. (2000), "A theoretical extension of the technology acceptance model: Four longitudinal field studies", *Management Science,* vol. 46, no. 2, pp. 186-204

Venkatesh, V., Morris, M. G., Davis, G. B. & Davis, F. D. (2003), "User acceptance of information technology: Toward a unified view", *MIS Quarterly,* vol. 27, no. 3, pp. 425-478.

Williams, P. (2001). Information security governance. Information Security Technical Report, 6, 60–70. http://dx.doi.org/10.1016/S1363-4127(01)00309-0.

Williams, P. (2008). In a 'trusting' environment, everyone is responsible for information security. Information Security Technical Report, 13, 207–215. http://dx.doi.org/10.1016/j.istr.2008.10.009.

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. Information Systems Security, 16, 315–331. http://dx.doi.org/10.1080/1065890701788165.

Yoh, E., Damhorst, M. L., Sapp, S. & Laczniak, R. (2003), "Consumer adoption of the internet: The case of apparel shopping", *Psychology & Marketing,* vol. 20, no. 12, pp. 1095-1118.