Information Security Policy Compliance: The Role of Information Security Awareness

Ahmad Al-Omari
College of Business and Information Systems, Dakota State University, Madison, SD, United States., Ahmad.Al-Omari@dsu.edu

Omar El-Gayar
College of Business and Information Systems, Dakota State University, Madison, SD, United States., omar.el-gayar@dsu.edu

Amit Deokar
College of Business and Information Systems, Dakota State University, Madison, SD, United States., Amit.Deokar@dsu.edu

Recommended Citation

Al-Omari, Ahmad; El-Gayar, Omar; and Deokar, Amit, "Information Security Policy Compliance: The Role of Information Security Awareness" (2012). *AMCIS 2012 Proceedings*. 16.
http://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/16

Information Security Policy Compliance: The Role of Information Security Awareness

Ahmad AL-Omari
Dakota State University
Madison, SD
Ahmad.Al-Omari@dsu.edu

Omar El-Gayar
Dakota State University
Madison, SD
Omar.El-Gayar@dsu.edu

Amit Deokar
Dakota State University
Madison, SD
Amit.Deokar@dsu.edu

ABSTRACT

Compliance and systems misuse has been the focus of researchers in the last couple of years. However, given that voids in this area is still significant and systems abuse is a pressing issue likely to persist in the future, more investigation is needed in this area. Toward this end, we conducted a research study to help understand factors motivating compliance behavior intentions. Drawing on Theory of Planned Behavior, we investigated the role of users' self-learning and knowledge of security issues in shaping their attitudes toward compliance with information security policies (ISPs). We collected data from nine financial organizations to test the proposed research model. Results show that employees' previous knowledge of security issues and technologies have significant positive impact on their attitudes toward compliance with ISPs. This study sheds light on the importance of users' general awareness of security issues and technologies in shaping their attitudes to comply with ISPs.

Keywords:

Information security awareness, compliance, information security policies, technology awareness, theory of planned behavior.

INTRODUCTION

Violations of information security policies (ISPs) have been shown to significantly increase information security threats and vulnerabilities, ultimately leading to information security breaches (Dhillon & Moores, 2001; Vance, 2010). As such, compliance with ISPs has become a key concern for organizations. ISPs must be designed by incorporating the necessary guidelines and instructions to familiarize employees with the rules and expected conduct while using organizational information and technology resources (Straub, 1990; Whitman, Townsend, & Aalberts, 2001). Although good design of ISPs is an essential step toward ensuring compliance, it does not address behavioral factors related to compliance. Accordingly, it is imperative to define and understand factors that motivate and enhance employees' compliance with ISPs.

Recently, more attention has been directed toward the human side of computer abuse, as a more important step towards effective information security management (Hu, Xu, Dinev, & Ling, 2010; Lee, Lee, & Yoo, 2004). The proposed research study builds on previous research by capturing the effects of users' self-learning and awareness of security issues on compliance behavior. Specifically, the study addresses the following research questions:

1. What is the role of employee's general knowledge of information security issues and technologies in forming his/her behavior toward compliance with ISPs?
2. What is the role of social pressure on employee's compliance intention with ISPs?
3. What is the role of self-efficacy on employees' compliance intention with ISPs?

The paper is organized as follows. In the next section, we review pertinent literature and highlight the research gaps addressed through this study followed by a description of the proposed research model and hypotheses. Next, we describe the research methodology, survey instrument, sample, and data collection method. The Data Analysis and Results section summarize the results obtained followed by a discussion of findings and limitations of the research study. Finally, the conclusion section highlights the theoretical and practical contributions of the research and concludes the paper.

LITERATURE REVIEW

A plethora of research has been conducted to explore the "negative" or improper computing behavior in the last years. The majority of the information security research to understand employees' misconduct or misuse and even criminal acts toward the organization's IT systems, has been conducted from different theoretical lenses (Hu et al., 2010). General deterrence theory has been one of the most prominent theories used to study employees' behavior, given that employee misconduct or misuse of organizational information systems and resources is related to criminal behavior (D'Arcy, Hovav, & Galletta, 2009; Hu et al., 2010; Kankanhalli, Teo, Tan, & Wei, 2003; Straub, 1990). Research studies have also adopted other theories such as Theory of Reasoned Acton (TRA), Theory of Planned Behavior (TPB), Rational Choice Theory (RCT), Protection Motivation Theory (PMT), Self-Control Theory (SCT), and Technology Acceptance Model (TAM) to study compliance behavior with ISPs and systems abuse or misuse (e.g. Posey, Roberts, Lowry, & Bennett, 2010; Siponen, Pahnila, & Mahmood, 2007; Siponen & Vance, 2010; Warkentin, Willison, & Johnston, 2011).We now review recent studies using the aforementioned theories. Straub (1990) argued that information security procedures can deter potential computer abusers from violating organizational policies. D'Arcy and Hovav (2009) adopted GDT to explore the moderating effect of computer self-efficacy and virtual status on perceptions of sanctions. Siponen and Vance (2010) argued that employees' violation of ISPs is not always best elucidated by fear of sanctions as employees may use neutralization techniques to reduce violation intention. Drawing on TPB, Bulgurcu, Cavusoglu, and Benbasat (2010) argued that information security awareness (ISA), and employee's attitude will determine compliance intention with ISPs. Li, Zhang, and Sarathy (2010) employed the RCT to examine factors influencing compliance of Internet use policies. In their research study, Siponen et al. (2007) combined PMT with GDT and TRA to explain how employees' compliance with ISPs can be improved. Herath and Rao (2009b) adopted PMT and GDT to test compliance intention by incorporating threat appraisal and coping appraisal constructs in their models to explain attitudes towards security policies. Zhang, Reithel, and Li (2009) adopted the TPB to examine impact of technical protection mechanisms on compliance intention. Anderson and Agarwal (2010) employed PMT along with TRA, and TPB to examine behavioral intentions to engage in security-related behavior. Johnston and Warkentin (2010) examined the influence of fear appeals on end users' intention to perform recommended individual computer security actions. Al-Omari, El-Gayar, and Deokar (2012) combined the TAM and TPB to investigate the impact of structured and unstructured ISA on intention to comply with the banks' ISPs. Siponen, Pahnila, and Mahmood (2010) proposed a model based on PMT, GDT, and TRA to help understand why some employees comply with their organizations' ISPs and why others do not. Drawing on TPB, Bulgurcu, Cavusoglu, and Benbasat (2009) investigated the role of employees' ISA in shaping their attitude toward intention to comply with ISPs. Kankanhalli et al. (2003) built a model based on GDT to test the effect of deterrent and preventive measures besides organizational factors on IS security effectiveness. Dinev and Hu (2007) used TPB and TAM constructs with technology awareness to study their effect on intention to use protective technologies.

A thorough review of the literature indicates that only two studies (e.g. Bulgurcu et al., 2010; Goodhue & Straub, 1991) examine, along with other factors, the role of users' personal knowledge built from life experiences and gained from different resources such as the Internet, newspapers, and security publications in shaping the users' compliance intention with ISPs. Goodhue and Straub (1991) were among the first scholars to denote the importance of awareness as an important factor in forming users' beliefs about information security. They note that computer abuse is a key problem that will not dwindle on its own, because "a lack of awareness of the danger may lead to weak vigilance by users and greater potential for abuse" (p. 14). Goodhue and Straub (1991) related awareness to computer literacy and, hence, defined awareness as years of experience, managerial level, and user/systems staff status. No study was found to address the role of self-awareness of information security issues and technologies *per se* as factors articulating employee's behavioral intention toward compliance with ISPs. In this study, we complement existing research by focusing on the role of employee's general knowledge awareness of information security issues in forming his/her behavior toward compliance with ISPs.

RESEARCH MODEL AND HYPOTHESES

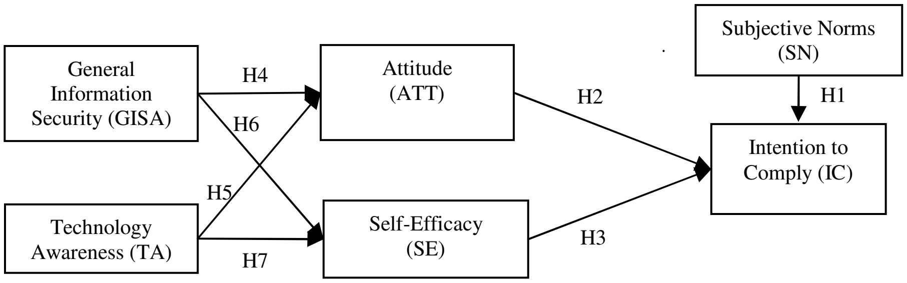

Figure 1. Research Model

Drawing on Ajzen's (1991) TPB as a theoretical basis, we propose a model that intends to explain employees' intention to comply with ISPs (Figure 1). Table 1 presents definitions of the TPB and study constructs and their sources. Relationships among TPB constructs have been extensively tested in the security compliance and systems misuse literature. Based on this foundation, we postulate that an employee's intention to comply with an organization's ISPs is affected by subjective norms, self-efficacy and attitude toward compliance. Self-efficacy is used instead of perceived behavioral control as it captures the same latent factor (Fishbein, 2008). This can be summarized in the form of following hypotheses:

Hypothesis H1: An employee's subjective norm about complying with the organization's ISPs positively affects intention to comply with the requirements of ISPs.

Hypothesis H2: An employee's attitude toward complying with the organization's ISPs positively affects intention to comply with the requirements of ISPs.

Hypothesis H3: An employee's self-efficacy related to complying with the organization's ISPs positively affects intention to comply with the requirements of ISPs.

Construct	Definition	Source
Intention to Comply	An employee's intention to protect the information and technology resources of the organization from potential security breaches	(Ajzen, 1991; Bulgurcu et al., 2010)
Attitude toward compliance	The degree to which the performance of the compliance behavior is positively valued	(Bulgurcu et al., 2010)
Self-efficacy	An employee's confidence in their ability, skills, and knowledge about satisfying the requirements of ISPs.	(Ajzen, 1991; Pavlou & Fygenson, 2006)
General Information Security Awareness	An employee's self-learning knowledge obtained by personal effort from the Internet, magazines, experience and other sources and understanding of potential issues related to information security and their ramifications.	(D'Arcy et al., 2009; Straub, 1990)
Technology Awareness	A user's raised self-consciousness of and interest in knowing about technological issues and strategies to deal with them obtained by personal effort from the Internet, magazines, and other resources.	(Dinev & Hu, 2007)
Subjective Norms	An employee's perceptions of social pressure about compliance with the requirements of the ISP caused by behavioral expectations of such important referents as executives, colleagues and managers.	(Bulgurcu et al., 2010) (Ajzen, 1991)

Table 1: Definitions and Sources of Constructs

Further, in the research model shown in Figure 1, it is posited that information security awareness about different security issues such as ISP, threats, protective technologies and controls influences employees' attitude toward compliance. Information Security Awareness is defined as an "employee's overall knowledge and understanding of potential issues related to information security and their ramifications" (Bulgurcu et al., 2010, p. 532). General Information Security Awareness (GISA) and Technology Awareness (TA) are two key dimensions of ISA.

General information security awareness is defined as "an employee's knowledge and understanding of potential issues related to information security and their ramifications" (Bulgurcu et al., 2009, p. 2). Employees are expected to be aware and knowledgeable of information security and cognizant of security technology and be able to formulate a general perception of what it entails. This definition is consistent with the belief that ISA is used to "refer to a state where users in an organization are aware of and ideally committed to their security mission" (Siponen, 2000, p. 31). Accordingly, organizations are expecting their employees to be having basic knowledge of security issues, which will be reflected in their work and in dealing with ISPs.

Dinev and Hu (2007) defined technology awareness as a "user's raised consciousness of and interest in knowing about technological issues and strategies to deal with them" (p.391). It seems logical for employees to be aware of various technological issues surrounding compliance with ISPs before they form either negative or positive beliefs about it. Dinev and Hu (2007) argue that employees must make themselves aware of potential threats and how compliance with ISPs can help protect information assets. Along similar vein, they must also be aware of the consequences of noncompliance, as well as the availability and effectiveness of protective technology (Dinev & Hu, 2007).

General information security awareness and technology awareness can be explained in the framework of innovation-decision process depicted in the innovation diffusion theory (Rogers, 1995), in which knowledge influences persuasion, which, in turn, influences decisions. In this context, ISA can be viewed as knowledge, attitude can be viewed as a form of persuasion, and intention to comply can be viewed as a decision. Building on this process, employees can gain significant "awareness knowledge" about different information security threats and protective technologies, in addition to knowledge about what and how they are supposed to do with regard to information security, which will consequently lead to compliance behavior (Bulgurcu et al., 2010). Accordingly, knowledge of information security threats can be viewed as general information security awareness, and knowledge about what employees are supposed to do can be viewed as technology awareness. It is thus posited that the information security awareness (knowledge) influences perceptions of attitude (persuasion), which in turn influences the intention (decision) to comply with the ISPs. The corresponding hypotheses are:

Hypothesis H4: An employee's general information security awareness positively affects attitude toward complying with the requirements of ISPs.

Hypothesis H5: An employee's technology awareness positively affects attitude toward complying with the requirements of ISPs.

Furthermore, Bandura (1977) defined knowledge and experience obtained indirectly as vicarious experience, and identified it as a source of self-efficacy (SE). Bandura (1977) argument was built on employees' expectations derived from observing others performing their work. In other words, employees' persuade themselves that if others can do it, so can they. According to Gist (1987), vicarious experience is more effective when models succeed after overcoming difficulty, and its effects are enhanced when the modeled behavior produces clear results or consequences. Therefore, the visibility of professional peers successfully overcoming difficulties with security issues by utilizing their experience, knowledge, and self-learning can be instrumental in persuading employees to enhance their general and technology awareness. Based on this argument, we posit that employees' general knowledge and experience of security related issues obtained indirectly (obtained through Internet, magazines, experience and other sources) will enhance their perceptions of their own performance capabilities, i.e. self-efficacy. This is summarized in our hypotheses as follows:

Hypothesis H6: An employee's general information security awareness positively affects his/her performance capabilities perceptions (self-efficacy) toward complying with the requirements of ISPs.

Hypothesis H7: An employee's technology awareness positively affects his/her performance capabilities perceptions (self-efficacy) toward complying with the requirements of ISPs.

METHODOLOGY

Setting, Subjects, and Data Collection

To test our hypotheses, we adopted survey research methodology. The survey study was conducted in nine different banks in Jordan. The subjects of the study are individuals employed in Jordanian banks drawn from various functional departments (teller, administrative/clerical, information technology, auditing, marketing and sales, credit departments and Treasury & investment). Surveys were randomly distributed to 2117 employees in nine different banks in Jordan. Given that English is a second language in Jordan, we took additional steps to avoid loss of meaning and included only those participants in the subsequent analysis who reported to be fluent in English. Based on this criterion, 878 subjects successfully completed the survey study.

Survey Instrument

For administering the survey, the survey instrument was developed based on constructs validated and tested in prior research (Bulgurcu et al., 2010; Dinev & Hu, 2007; Herath & Rao, 2009a; Siponen et al., 2010), standardized and adapted to the context of this study. The survey instrument was refined based on the feedback obtained from information security researchers in United States and Jordan as well as from knowledge workers at several banks in Jordan. A pilot study was conducted to measure the validity and reliability of the instrument. A pilot study was conducted on a convenience sample of 205 employees from four different banks in Jordan. The pilot test was analyzed and the instrument was found to be valid and reliable (reference will be added after the review process). In addition to the constructs noted in Figure 3, the instrument also collected additional demographic information including gender, age, length of computer experience, and average computer usage per day.

Data Analysis

The component-based partial least squares (PLS) approach, a structural modeling technique, was used to test and evaluate the psychometric properties of the constructs and to test the study hypotheses. PLS was chosen as the data analysis technique since it is better than traditional first generation statistical methods (e.g., regression) in that it tests the measurement model (relationships between constructs and measurement indicators) and the structural model (theoretical relationships among constructs) simultaneously. In performing the analysis, PLS technique estimates item loadings on constructs (outer model) and then estimates path coefficients for casual relationships among constructs iteratively (inner model) (Gefen, Straub, & Boudreau, 2000). PLS, as a component-based approach is commonly used in Information Systems research as it (a) allows analysis of non-normal data, (b) is less sensitive to sample size issues, supports exploratory research (Gefen et al., 2000), (c) helps conduct high quality theory-testing (Rouse & Corbitt, 2008), and (d) processes each indicator separately which allows each item to differ in the amount of influence on the construct estimate (Chin, Marcolin, & L., 2003). PLS is considered most appropriate for this study because of its focus on prediction, and suitability for exploratory research and theory building. The SmartPLS software package (version 2.0.M3) (Ringle, Wende, & Will, 2005) was used to assess the measurement model fit indices and evaluate the validity and reliability.

RESULTS, DISCUSSION AND FUTURE WORK

Sample Characteristics

Figure 4 in the Appendix summarizes respondents' descriptive statistics. Of the 878 respondents in the final sample, 44% were female, 19.9% were in the 20-29 age range, 62.8% held a bachelor's degree, and 54.6% had 1-5 years of experience. The average computer usage experience (using different computer software such as spreadsheet, word processing, e-mail, programming languages, database applications and bank's special tailored software) was noted to be 9.93 years, and the average use of computer at work was noted to be 6.29 hours per day.

Instrument Validity

As noted earlier, the survey instrument is based on constructs validated and tested in prior research (Al-Omari et al., 2012; Bulgurcu et al., 2010; Dinev & Hu, 2007; Herath & Rao, 2009a, 2009b; Siponen et al., 2010), standardized and adapted to the context of this study. Guidelines presented by Straub (Straub, 1989) indicate that using validated and tested items will improve the reliability of results. Using SmartPLS software package (version 2.0.M3) (Ringle et al., 2005), we assessed the convergent validity, discriminant validity, and reliability of the survey instrument. 30 variables initially included in the instrument were examined to scrutinize any item loadings less than 0.70, as recommended (Straub, 1989). Figure 5 summarizes the items constituting the research model. All 6 factors accounted for 68.7% of the total variance.

To ensure convergent validity and reliability of the survey instrument, factor loadings of each individual item on their underlying construct were examined as well as the Average Variance Extracted (AVE). As can be seen from Figure 5, all item loadings exceeded the recommended minimum value of 0.70, indicating that at least 50 percent of the variance accounted for by the construct (Hair, Black, Babin, Anderson, & Tatham, 2009). As shown in Table 2 the AVE was higher than the minimum recommended value of 0.5 for each construct indicating that the items satisfied the convergent validity.

	Cronbach's alpha	CR	AVE	ATT	GISA	IC	SE	SN	TA
ATT	0.930	0.947	0.782	0.884					
GISA	0.908	0.942	0.845	0.215	0.919				
IC	0.948	0.957	0.763	0.373	-0.042	0.873			
SE	0.939	0.952	0.766	0.342	0.253	0.289	0.875		
SN	0.936	0.951	0.795	0.302	0.252	0.369	0.356	0.892	
TA	0.915	0.940	0.797	0.270	0.213	0.305	0.298	0.289	0.893

CR = Composite reliability; AVE = Average Variance Extracted; ATT = Attitude; GISA = General Information Security Awareness;
IC = Intention to Comply; SE = Self-Efficacy to Comply; SN = Subjective Norms; TA = Security Awareness.
Diagonal elements in bold display the square root of AVE.

Table 2. Composite Reliability, AVE, and Latent Variable Correlations

To establish discriminant validity, both the loading and cross loading matrix (Figure 5) and the correlation matrix (Table 2) were examined. All measurement items loaded more strongly on their respective construct than on other constructs. Second, Table 2 shows that the square root of AVE of each construct is higher than the correlations between that construct and any other construct (inter-correlations) (Fornell & Larcker, 1981). As shown in Table 2 and Figure 5, all constructs in the model satisfy these criteria for discriminant validity. Consequently, our measurement model demonstrates adequate reliability and validity required for further testing of our research hypothesis.

To confirm the scale reliability and internal consistency, composite reliability (CR) and Cronbach's alpha was calculated. A scale is deemed to be reliable if it has CR and Cronbach's alpha above 0.70 (Gefen et al., 2000). Table 2 shows that all composite reliability values are more than 0.942 and Cronbach's alpha, are higher than 0.907, demonstrating that all constructs had the reflective scales were reliable.

Structural Model Testing Results

As stated in the Methodology section, PLS approach to structural equation modeling was used to estimate our measurement model. The PLS algorithm and the bootstrapping re-sampling method with 878 cases and 1756 re-sample were used to estimate the structural model. Figure 2 shows the results of the model estimation, path coefficients, path significance based on a two-tailed t-test, and the variance explained by the independent variables (R^2). Based on these results (Figure 2) all hypotheses were supported ($p < 0.001$). The structural model explained approximately 19.0 percent of the variance for the intention to comply, where 32.5 percent of the variance could be explained for attitude and 12.7 percent of the variance could be explained for SE.

There is no doubt that employees' compliance with ISPs is a key issue that management is trying to address in many organizations. Conceptually, employees who are aware of the ISPs instituted in their organizations, and yet deliberately violate these policies are certainly a significant security threat to the organization as awareness and training programs is likely to have little impact on their behavior (Siponen, 2000; Vance, 2010). Previous literature viewed this problem through various theoretical lenses and different models have been proposed. In this study we have utilized TPB to investigate the role of users' self-learning and awareness of security issues and security technologies on shaping their compliance intention. All hypotheses were supported based on data collected from 878 employees from nine different banks in Jordan.

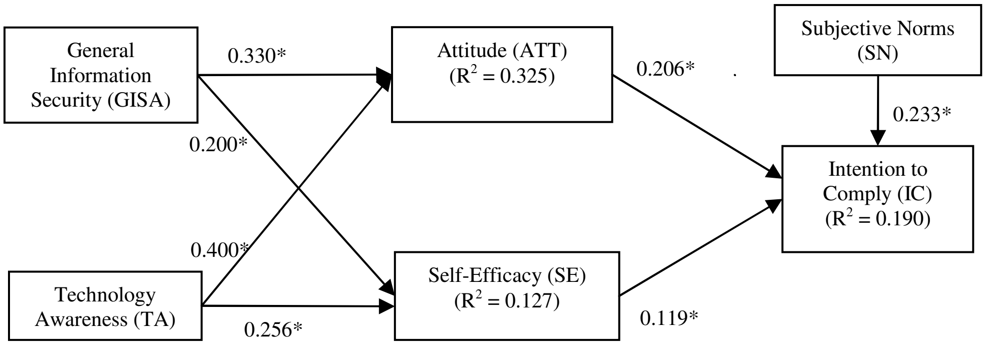
General Information Security (GISA)
Technology Awareness (TA)
Attitude (ATT) ($R^2 = 0.325$)
Self-Efficacy (SE) ($R^2 = 0.127$)
Subjective Norms (SN)
Intention to Comply (IC) ($R^2 = 0.190$)
0.330*
0.200*
0.400*
0.256*
0.206*
0.233*
0.119*

Figure 2. Results of the Structural Model Testing

As postulated in TBP, attitude was found to have significant impact on employees' intention to comply, explaining 24.1% of its variance. Thus, hypothesis 1 is fully supported. Also, subjective norm was found to have significant effect on intention to comply, explaining the highest variation (33.2%) of construct. Self-efficacy was found to have significant positive impact on intention to comply explaining 17.3% of the variance in compliance intention. Thus, hypotheses 2 and 3 are fully supported. Furthermore, as hypothesized, result shows that both GISA and TA have significant positive impact on employees' attitude toward compliance with ISPs, where GISA explained 32.9% and TA explained 35.9% of the variance in attitudes. Thus, hypotheses 4 and 5 are supported. Also, the results indicate that both GISA and TA have significant positive impact on employees' SE toward compliance with ISPs, where GISA explained 20.8% and TA explained 39.9% of the variance in SE. Thus, hypotheses 6 and 7 are supported as well. Table 3 summarizes the results of hypotheses testing.

Hypothesis	Hypothesis (Direction)	Path Coefficient	t-value	Significant	Supported?
H1	SN → IC (+)	0.233	5.233	P < 0.001	Yes
H2	ATT → IC	0.206	4.961	P < 0.001	Yes
H3	SE → IC (+)	0.119	3.104	P < 0.001	Yes
H4	GISA → ATT (+)	0.330	10.931	P < 0.001	Yes
H5	TA → ATT (+)	0.400	14.309	P < 0.001	Yes
H6	GISA → SE (+)	0.200	4.645	P < 0.001	Yes
H7	TA → SE (+)	0.256	5.961	P < 0.001	Yes

Table 3. Main Effect Path Coefficient (Structural Model Results)

As with any research, this study has some limitations that have to be noted in interpreting the results. One limitation of this study is related to the selection of participants. At the collection data process, employees were asked if they speak English fluently and if they are aware of the bank's ISPs. Those who did not satisfy any one of these requirements were excluded from the survey. This might have introduced a favorability bias in the response. Other limitations relate to the mechanics of the research study. Given that "intention" is a self-reported measure, we acknowledge that some employees might not have expressed their true intention for a variety of reasons. Another limitation is that the data was collected in a cross-sectional manner, which might lead one to measure a correlation rather than a causation effect. The researchers were not able to administer the questionnaire first hand and thus respond immediately to any unforeseen hurdles. The questionnaire was administered by some of the researchers' professional peers. This may be considered a limitation from survey administration perspective. Another research limitation may be the language barrier and the possible loss of meaning that might have occurred since English is a second language in Jordan, where data is gathered. However, we tried to mitigate this limitation by considering the responses of only those participants that were fluent in English.

CONCLUSION

Overall, this study is the first to address the role of users' general knowledge of information security issues on their attitude to comply with ISPs. The result suggests that an employee's attitude toward compliance with ISP can be enhanced by his/her general security awareness. As for employees' knowledge and understandings of security related technologies, it also found to have significant positive impact on attitude. This suggests that employees encompass enough knowledge, and have enough resources (e.g. magazines, discussion forum, and online help) about security issues which helped shape their behavior toward compliance with ISPs. Further, the results suggest that employees' knowledge of security related issues and technologies enhance their perceptions of their own performance capabilities to comply with ISPs. Overall, these findings imply that creating security-aware culture within the organization will shape users' attitude and behavior to be more security-conscious. As ISA is a key factor in compliance behavior, our findings are expected to provide a comprehensive picture of the factors that constitute ISA which will be helpful for practitioners in designing ISA programs. This study will contribute to the understanding of the theoretical background of existing IS security awareness approaches with a particular emphasis rooted in the users' perspective and knowledge. Future studies may incorporate other organizational factors such as organizational culture to the existing model.

REFERENCES

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179-211.

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). *Security Policy Compliance: User Acceptance Perspective*. Paper presented at the 2012 45th Hawaii International Conference on System Sciences, Maui, Hawaii.

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing Special Issue Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly, 34*(3), 613-643.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191-215.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009). *Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance.* Paper presented at the AMCIS 2009 Proceedings. Paper 419.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Chin, W., Marcolin, B., & L., N., P., R. (2003). A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study. *Information Systems Research, 14*(2), 189-229.

D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics, 89*(S1), 59-71.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research, 20*(1), 79-98.

Dhillon, G., & Moores, S. (2001). Computer crimes: theorizing about the enemy within. *Computers &amp; Security, 20*(8), 715-723.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems, 8*(7), 23.

Fishbein, M. (2008). A reasoned action approach to health promotion. *Medical Decision Making, 28*(6), 834.

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research, 18*(1), 39-50.

Gefen, D., Straub, D., & Boudreau, M. C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems, 4*(1), 7.

Gist, M. E. (1987). Self-Efficacy: Implications for Organizational Behavior and Human Resource Management. *The Academy of Management Review, 12*(3), 472-485.

Goodhue, D. L., & Straub, D. (1991). Security concerns of system users : A study of perceptions of the adequacy of security. *Information & Management, 20*(1), 13-27.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2009). *Multivariate Data Analysis* (Seventh Edition ed.). Upper Saddle River, NJ: Pearson Prentic Hall.

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

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

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2010). *Why Individuals Commit Computer Offences in Organizations: Investigating the Roles of Rational Choice, Self-Control, and Deterrence.* Paper presented at the Proceedings of the Pacific Asia Conference on Information Systems (PACIS), Paper 132.

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *Management Information Systems Quarterly, 34*(3), 549-566.

Kankanhalli, A., Teo, H. H., Tan, B. C. Y., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139-154.

Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management, 41*(6), 707-718.

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems, 48*(4), 635-645.

Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *Management Information Systems Quarterly, 30*(1), 8.

Posey, C., Roberts, T. L., Lowry, P. B., & Bennett, B. (2010). *How Explanation Adequacy of Security Policy Changes Decreases Organizational Computer Abuse.* Paper presented at the Proceedings of the Ninth Annual Workshop on HCI Research in MIS (SIGHCI), Paper 14, Saint Louis, Missouri.

Ringle, C. M., Wende, S., & Will, S. (2005). SmartPLS Release 2.0 (M3) Beta. University of Hamburg, Hamburg, Germany: http://www.smartpls.de.

Rogers, E. M. (1995). *Diffusion of innovations* (Fourth ed.). New York: The Free Press.

Rouse, A., & Corbitt, B. (2008). There's SEM and" SEM": A Critique of the Use of PLS Regression in Information Systems Research. *ACIS 2008 Proceedings*, 81.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: an empirical study. In H. Venter, Eloff, M., Labuschagne, L., Eloff, J., von Solms, R. (Ed.), *IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments* (pp. 133-144): Boston: Springer.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer, 43*(2), 64-71.

Siponen, M., & Vance, A. O. (2010). Neutralization: New Insights into the Problem of Employee Systems Security Policy Violations. *MIS Quarterly, 34*(3), 487-502.

Straub, D. (1989). Validating instruments in MIS research. *MIS Quarterly, 13*(2), 147-169.

Straub, D. (1990). Effective IS security. *Information Systems Research, 1*(3), 255-276.

Vance, A. (2010). *Why do employees violate is security policies? Insights from multiple theoretical perspectives.* (Ph.D.), University of Oulu, Department of Information Processing Science. (Dissertation)

Warkentin, M., Willison, R., & Johnston, A. C. (2011). *The Role of Perceptions of Organizational Injustice and Techniques of Neutralization in Forming Computer Abuse Intentions.* Paper presented at the AMCIS 2011 Proceedings - All Submissions. Paper 318.

Whitman, M. E., Townsend, A. M., & Aalberts, R. J. (2001). Information systems security and the need for policy. In G. Dhillon (Ed.), *Information Security Management: Global Challenges in the New Millennium*. Hershey, PA, USA: Idea Group Publishing.

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security, 17*(4), 330-340.

APPENDIX

Items	Dimensions/Questions
IC	**Intention to Comply**
	I intend to comply with the requirements of the ISP of my organization
	I intend to protect information resources according to the requirements of the ISP of my organization.
	I intend to protect technology resources according to the requirements of the ISP of my organization.
	I intend to carry out my responsibilities prescribed in the ISP of my organization when I use information resources.
	I intend to carry out my responsibilities prescribed in the ISP of my organization when I use technology resources.
	I intend to recommend that others comply with ISP.
	I intend to assist others in complying with ISP.
GISA	**General Information Security Awareness**
	Overall, I am aware of the potential security threats and their negative consequences
	I have sufficient knowledge about the cost of potential security problems.
	I understand the concerns regarding information security and the risks they pose in general.
TA	**Technology Awareness**
	I follow news and developments about the security related technologies.
	I discuss Internet security issues or anecdotes with friends and people around me
	I read about the problems of malicious threats attacking users' computers.
	I seek advice about security issues through online discussion forums, magazines, and other media sources
SN	**Subjective Norm**
	Upper level management thinks I should comply with the requirements of my organization's ISPs.
	My boss thinks that I should comply with the requirements of my organization's ISPs.
	My colleagues think that I should comply with the requirements of my organization's ISPs.
	The information security/technology department in my organization thinks that I should comply with the requirements of my organization's ISPs.
	Other computer technical specialists in the organization think that I should comply with the requirements of my organization's ISPs.
SE	**Self-Efficacy**
	I have the necessary skills to fulfill the requirements of the ISP.
	I have the necessary knowledge to fulfill the requirements of the ISP.
	I have the necessary competencies to fulfill the requirements of the ISP.
	I would feel comfortable following my organization's ISP on my own.
	If I wanted to, I could easily comply with my organization's ISP on my own.
	I would be able to follow most of ISP even if there was no one around to help me.
ATT	**Attitude: To me, complying with the requirements of my organization's ISP is**
	Not necessary.... Necessary
	Not beneficial.... Beneficial
	Not important.... Important
	Not useful.... useful
	Not exciting.... exciting

Figure 3. Measurement Items

	Item	Freq.	Percent
Gender	Male	492	56.0%
	Female	386	44.0%
Age	20-29 Years	605	68.9%
	30-39 years	175	19.9%
	40-49 years	66	7.5%
	≥ 50 years	32	3.6%
Education	High School	61	6.9%
	Collage	122	13.9%
	Bachelor's Degree	551	62.8%
	Master's Degree	119	13.6%
	Doctoral Degree	25	2.8%
Experience	1-5 years	479	54.6%
	6-10 years	181	20.6%
	11-15 years	72	8.2%
	16-20 years	95	10.8%
	More than 20 years	51	5.8%

Figure 4. Descriptive statistics of respondents

	ATT	GISA	IC	SE	SN	TA
ATT1	**0.884**	0.385	0.341	0.371	0.357	0.243
ATT2	**0.859**	0.351	0.284	0.438	0.322	0.381
ATT3	**0.898**	0.364	0.340	0.217	0.360	0.323
ATT4	**0.882**	0.370	0.328	0.482	0.351	0.308
ATT5	**0.896**	0.363	0.352	0.487	0.329	0.220
GISA1	0.362	**0.882**	-0.024	0.211	0.206	0.194
GISA2	0.421	**0.922**	-0.068	0.242	0.262	0.230
GISA3	0.354	**0.952**	-0.017	0.244	0.222	0.158
IC1	0.270	-0.054	**0.885**	0.196	0.324	0.222
IC2	0.286	-0.038	**0.885**	0.205	0.316	0.238
IC3	0.319	-0.052	**0.889**	0.244	0.321	0.251
IC4	0.338	-0.029	**0.881**	0.242	0.344	0.262
IC5	0.355	-0.044	**0.882**	0.259	0.317	0.262
IC6	0.343	-0.030	**0.856**	0.273	0.306	0.328
IC7	0.354	-0.011	**0.835**	0.327	0.326	0.290
SE1	0.461	0.190	0.252	**0.862**	0.308	0.281
SE2	0.396	0.215	0.233	**0.882**	0.301	0.283
SE3	0.377	0.233	0.218	**0.875**	0.270	0.261
SE4	0.253	0.226	0.274	**0.895**	0.336	0.239
SE5	0.275	0.228	0.234	**0.867**	0.315	0.238
SE6	0.388	0.238	0.290	**0.869**	0.328	0.263
SN1	0.250	0.253	0.327	0.302	**0.891**	0.260
SN2	0.252	0.268	0.300	0.322	**0.888**	0.240
SN3	0.346	0.184	0.322	0.301	**0.896**	0.272
SN4	0.339	0.215	0.349	0.339	**0.902**	0.241
SN5	0.253	0.210	0.344	0.321	**0.881**	0.272
TA1	0.387	0.152	0.268	0.238	0.268	**0.889**
TA2	0.244	0.228	0.233	0.289	0.242	**0.901**
TA3	0.399	0.186	0.301	0.258	0.264	**0.890**
TA4	0.243	0.192	0.289	0.274	0.259	**0.892**

Figure 5. Measurement Items and Item Loadings