2012

Security policy compliance: User acceptance perspective

Ahmad Al-Omari
Dakota State University

Omar F. El-Gayar
Dakota State University

Amit Deokar
Dakota State University

Recommended Citation

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012, January). Security policy compliance: User acceptance perspective. In 2012 45th Hawaii International Conference on System Sciences (pp. 3317-3326). IEEE.

2012 45th Hawaii International Conference on System Sciences

Security Policy Compliance: User Acceptance Perspective

Ahmad Al-Omari
Dakota State University
Ahmad.Al-Omari@dsu.edu

Omar El-Gayar
Dakota State University
Omar.El-Gayar@dsu.edu

Amit Deokar
Dakota State University
Amit.Deokar@dsu.edu

Abstract

Information security policy compliance is one of the key concerns that face organizations today. Although, technical and procedural security measures help improve information security, there is an increased need to accommodate human, social and organizational factors. While employees are considered the weakest link in information security domain, they also are assets that organizations need to leverage effectively. Employees' compliance with Information Security Policies (ISPs) is critical to the success of an information security program.

The purpose of this research is to develop a measurement tool that provides better measures for predicting and explaining employees' compliance with ISPs by examining the role of information security awareness in enhancing employees' compliance with ISPs. The study is the first to address compliance intention from a users' perspective. Overall, analysis results indicate strong support for the proposed instrument and represent an early confirmation for the validation of the underlying theoretical model.

1. Introduction

Modern organizations are heavily reliant on technology to uphold their information in electronic forms that are very vulnerable to attack, either from inside or outside. Consequently, securing information assets and data protection has become a major concern and challenge facing organizations and customers. Despite the large amounts of effort and expenditure of funds by organizations to secure their assets, many incidents of data breaches and information loss continue to happen every year [1]. To secure information assets and to reduce the risk associated with these systems, organizations typically concentrate on technical and procedural security measures [2]. Although these solutions help improve information security [3], relying on them alone is not enough to eliminate risk [4] and so human, social and organizational factors must be considered as well [5].

Adding to the need to design effective security policies [6, 7], is a concomitant necessity to enhance users' security awareness to comply with these information security policies [8], and this has led information security researchers to focus on the human and organizational factors to secure information resources [2, 4, 9, 10]. Even though the creation of comprehensive information security policies (ISPs) and guidelines concerning employee governance and behavioral control with regards to implementing secure practices has been given high priority, compliance with these policies is still lacking. Therefore, identifying the factors that motivate employees' awareness to comply with their organization's ISP is an important step toward helping information security managers understand and solve behavioral and managerial issues in information security management.

Most of the security awareness programs available to date may not be effective to fill the gap between perception and behavior [11]. Some researchers including Valentine [12] believe that this gap is due to the lack of a pre-defined methodology to deliver these programs. In order to address this gap, attention has been directed toward deploying behavioral theories to understand and direct users' behavior to be more security-conscious [e.g. 13, 14].

Some recent studies have investigated employees' compliance behavior from different perspectives. Bulgurcu, et al., [4] traced employees' attitudes toward compliance with ISPs back to an underlying set of compliance-related beliefs derived from Rational Choice Theory (RCT). Herath and Rao [15] have investigated motivational factors rooted in Protection-Motivation Theory (PMT), General Deterrence Theory (GDT) and organizational behavior to examine the adoption of ISPs and practices. Siponen and Vance [16] have argued that neutralization techniques influence employees' intention to violate ISPs.

Drawing on the technology acceptance model [17], it is posited that employees' intention to comply with the organization's ISPs is influenced by Perceived Ease of Use of ISPs (PEOU) and Perceived Usefulness of Protection (PUOP) afforded through the use of ISPs. The role of Perceived Behavioral Control (PBC) antecedents to PEOU and PUOP, namely self-efficacy and controllability, which in turn are rooted in the

978-0-7695-4525-7/12 $26.00 © 2012 IEEE
DOI 10.1109/HICSS.2012.516

Theory of Planned Behavior (TPB) [18], have also been considered. Finally, the role of information security awareness has been investigated and it is postulated that it will influence employees' PEOU of ISPs and PUOP provided by the policies leading to compliance with the ISPs.

The purpose of this research is to develop a measurement tool that provides better measures for predicting and explaining employees' compliance with ISPs by examining the role of information security awareness in enhancing employees' compliance with ISPs. The primary investigation focuses on developing the main constructs, PUOP and PEOU. Background factors will be explored. These include self-efficacy, controllability, subjective norms, and users' awareness of information security, security policies, security education, training and awareness program (SETA), and computer monitoring. Largely, derived from previous literature; they are validated and tested in different research settings. Definitions of the constructs are formulated and the theoretical rationale for their hypothesized influence on ISP compliance is explained. Multi-item measurement scales for constructs are developed, pretested and then validated.

The rest of the study is arranged as follows. The next section presents a brief review of the relevant literature and highlights the gaps that this study aims to address. Section 3 presents the theoretical foundations, discusses the research model, and research hypotheses to be tested. Section 4 describes the research methodology, survey instrument, sample, and data collection method. Section 5 presents the data analysis and results. Finally, the article concludes with Section 6 highlighting the contributions, limitations and future directions of this research.

2. Literature Review

Information Security researchers and practitioners have increased their emphasis toward individual and organizational perspectives to enhance employees' compliance with ISPs [3, 4, 19], which has emerged as a key socio-organizational resource [4, 7, 8] to prevent and reduce information system resources misuse and abuse by insiders [3]. Studies that investigate end-user behavior argue that employees often willingly choose to misuse or abuse the system [4]. Most information security empirical studies have tried to apply GDT as a way to reduce this problem [3, 10, 20].

Straub [3] found that different preventive and deterrent techniques are effective for IS security. Kankanhalli, et al., [20] found that greater deterrent effort appears to contribute to better IS security effectiveness, while enforcing more severe penalties does not seem to prevent IS abuses. Similarly, Pahnila, et al., [21] found that sanctions do not have an effect on employees' intentions to comply with ISPs. In contrast to that, Herath and Rao [15] found that severity of penalty has a negative effect on employees' intention to comply with ISPs.

Other studies employed different theories to enhance employees' compliance with ISPs and reduce systems misuse. Based on the TPB, Dinev and Hu [14] found that higher awareness leads to higher confidence in preventing negative technologies (such as computer viruses, spyware). Drawing on TPB and RCT, Bulgurcu, et al [4], found that attitude, normative belief, and self-efficacy have a significant effect on employees' intention to comply with ISPs. Anderson and Agarwal [22] employed PMT along with the Theory of Reasoned Action (TRA) and TPB and found that home computer users' intentions to perform security-related behavior are influenced by a combination of cognitive, social, and psychological factors. Siponen and Vance's model is based on the Neutralization Theory and GDT [16], and they found that neutralization is an excellent predictor of employees' intention to violate ISPs. Developing their model based on the PMT, Johnston and Warkentin [23] found that 'fear appeal' is a positive predictor of a user's behavioral intention to comply with recommended individual security acts.

Using the Technology Acceptance Model (TAM), Dinev and Hu [14] found that PUOP and PEOU have no significant effect on users' intention to use protective technologies. Jones [24] found that PUOP and Subjective Norms (SN) are significant predictors of employees' behavioral intention to use security controls.

Security awareness education and training was and continues to be one of the most important fundamentals to information security practices [9, 11]. Puhakainen and Siponen [9] proposed a training program based on the Universal Constructive Instructional Theory and found that training programs are needed to enhance employees' ISP compliance. D'Arcy, et al., [10] found that users' awareness of security controls reduced IS misuse intentions. Bulgurcu, et al., [4] found that information security awareness has a strong effect on an employee's attitude to comply with the ISP.

To enforce compliance with information security policy, Pahnila, et al., [21] found that information quality, facilitating conditions, and habits, have a significant effect on employees' compliance with ISPs. Greene and D'Arcy [25] found that job satisfaction and security culture, and computer monitoring, lead to increased compliant security behavior. Siponen, Pahnila, & Mahmood [26] found that rewards are negatively related to actual compliance with ISPs.

A thorough analysis of the previous literature discussed above shows various behavioral theories have been employed to study employee attitudes towards compliance with ISPs and efforts to prevent systems misuse and abuse. While these studies have highlighted either the deterrent effect of sanctions or the role of incentives in encouraging employees' desirable behavior, none of the studies have addressed this problem from a system perspective by conceptualizing ISPs as a system that employees must accept first, as Davis [27] did with the ordeal of accepting a technology. Based on the analysis of the extant literature, it is evident that existing theoretical developments have been effective in defining the factors that enhance compliance or prevent system abuse. However, one of the major limitations of the research thus far is that it addresses the research problem only from an organizational perspective, not considering the users' perspective. To address this gap, this research project aims to develop a Security Acceptance Model (SAM), motivated by the TAM, to understand how information security awareness will enhance employees' compliance with ISPs by increasing the degree to which they perceive putting ISPs into practice and engaging in the corresponding roles and responsibilities as relatively effortless (PEOU), and also bolstering their belief that using these roles and responsibilities to safeguard the organization's information technology resources will help their job duties and performance (PUOP).

In developing our research model, we considered different existing behavioral theories that can be built upon. In that regard, TRA, TPB, RCT, and TAM were considered as candidate theories because each of them has the potential to predict behavioral intention. TRA and TPB, its extension, is a general model and, *per se*, does not specify the beliefs that are operative for a particular behavior. RCT posits that the individual's decision to engage in a criminal behavior is a function of his perceptions of cost and benefits of deviant behaviors in deciding whether to offend [28, 29]. RCT criticism often stems from the confusion surrounding many of its key concepts, premises, and predictions [4, 28]. Therefore, SAM is expected to possess all of the TAM's distinctiveness and is anticipated to be easy, simple, valid, and applicable in different cultures as well as with all forms of ISPs Finally, it can be used to understand users' compliance behavior.

3. Research Model

The proposed Security Acceptance Model is shown in Figure 1. It is aimed at helping explain employees' intention to comply with ISPs. With the recognition that ISPs are systems that users will use and comply with, SAM is built on the premise that the greater the readiness of the users to accept new system, the more likely they are to make changes in their practices, and the more willing they are to spend the time and effort to actually start using the system. In that regard, we draw on Bulgurcu, et al. [4] for their definition of information security policy as a "state of the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations" (p. 527).

This study will examine the effect of external variables on PUOP and PEOU of ISPs. These variables include: perceived security protection mechanisms (user awareness of security policies, SETA programs, and computer monitoring) proposed and tested by Straub [3], D'Arcy, et al. [10], and D'Arcy and Hovav [30], controllability [13, 14], information security awareness [4] and self-efficacy [14]. Information security awareness is posited to directly influence employees' PUOP toward compliance with ISPs [4]. The original relations in the model are posited to impact a user's behavioral intention to comply. Discussed below is the operationalization of the research constructs.

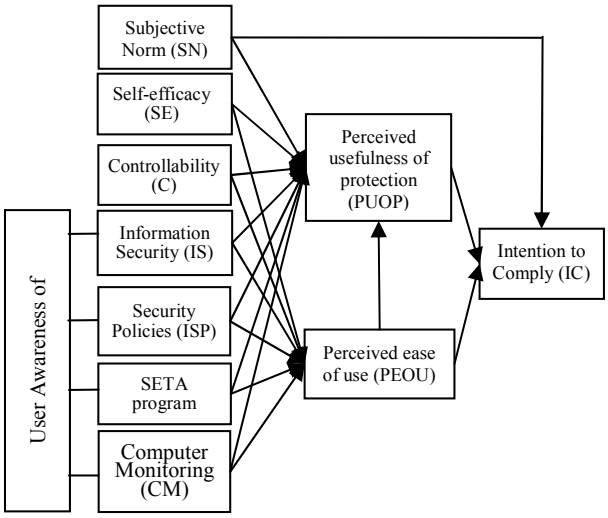

Figure 1: Research Model - Security Acceptance Model (SAM)

3.1 Perceived Usefulness of Protection (PUOP) and Perceived Ease of Use (PEOU)

In accordance with the existing literature, particularly TAM, it is assumed that an employee's intention to comply with the requirements of the organization's ISPs is associated with the degree to which the employee believes that using ISPs' roles and responsibilities to safeguard the organization's information technology resources will enhance their

job performance (PUOP). Also, it is associated with the degree to which an employee believes that using ISPs' in practice and undertaking related roles and responsibilities is relatively easy (PEOU). According to TAM, perceived usefulness is defined as "the degree to which an individual believes that using a particular system would enhance his or her job performance" [31], and perceived ease of use is defined as "the degree to which a person believes that using a particular system would be free of effort" [31], whereas, intention to comply is defined as an "employee's intention to protect the information and technology resources of the organization from potential security breaches" [4].

3.2 Subjective Norm

Under the assumptions of TRA, the intention to perform a behavior is a function of attitudes toward the behavior and social influence represented by subjective norms [32]. A Subjective norms (SN) has been defined as "the person's perception of social pressure to perform or not perform the behavior under consideration" [32]. Davis et al. [17] does not include SN in TAM as it is the least understood aspect of TRA, besides which it is assumed that computer use is voluntary. Despite that, many studies incorporated the construct thereafter, and it was found to have a significant effect on intention in mandatory settings but not in voluntary settings [33-35]. Venkatesh and Davis [34] refer to the causal mechanism underlying this effect as compliance. They posit that the direct compliance effect of SN on intention is theorized to operate whenever a person perceived that an important referent(s) wants him to perform a specific behavior, and that referent(s) has the ability to reward behavior or punish non-behavior.

3.3 Self-Efficacy and Controllability

Controllability (C) and self-efficacy (SE) are separable components of *Perceived* Behavioral Control (PBC) [18], which will allow more detailed examination of external control beliefs [36]. They can reflect internal as well as external factors [18].

Self-efficacy is a construct that has been examined in an exploratory sense in studies pertaining to an individual's use of IS and was found to be a significant predictor of behavioral intention [13]. Self-efficacy is defined as a "subjective probability that one is capable of executing a certain course of action" [32]. Consistent with this definition and in line with the study's purposes, self-efficacy is defined as an employee's confidence in their ability, skills, and knowledge with respect to satisfying the requirements of ISPs. Studies found that self-efficacy has a significant effect on the PEOU [37] and on PU (in this case PUOP) [38].

Controllability is defined as "individual judgments about the availability of resources and opportunities to perform the behavior" [18, 36]. The definitions of SE and C revealed that SE reflects internal personality factors, while controllability reflects beliefs about external factors [14]. According to Ajzen [18], some studies employed either one item or a mixture of both items, and debate surrounding the conceptualization of SE and C and their relationship to PBC still exists [39]. Previous studies have demonstrated the combined set to be a better predictor of intentions [18]. Controllability is found to be significant in predicting behavior but not intentions, while self-efficacy is found to be significant in predicting intentions [18]. As such, we use both self-efficacy and controllability in our study. Relationships between controllability and PU and PEOU have been examined in past studies Kim, Park and Oh [40] found C to have an indirect impact on a respondent's continued intention to use through its impact on PEOU [40].

3.4 Information Security, Security policies, SETA Program and Computer Monitoring

Goodhue and Straub [41] first noted the importance of awareness as an important factor in users' beliefs about information security. They believe 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). They also argued that "people who are more aware of the potential for abuse would be sensitized to the dangers of inadequate security and would more likely feel that security was unsatisfactory" (p. 14). Information Security Awareness (ISA) is defined as an "employee's overall knowledge and understanding of potential issues related to information security and their ramifications" [4]. 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 coherent 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" [42].

An individual's awareness and knowledge of information security is built from life experiences, such as having been attacked by a virus, opening unknown emails, being penalized for not complying with security policies and regulations, or obtaining information from external resources such as the Internet, newspapers, or security journals [4, 41]. Fishbein [43] argues that there are an infinite number of variables that may directly or indirectly influence the performance (or nonperformance) of any behavior. TPB posits that background factors (e.g. social,

demographic, experience, knowledge, values) may be related to or influence behavior indirectly by affecting behavioral, normative, and control beliefs [44]. In this context we can argue that an employees' ISA, conceived as a background factor, may prompt further development of his outcome beliefs when accompanied with compliance behavior.

Security policies, SETA programs and computer monitoring were identified as countermeasures that can be used by organizations to deter information systems misuse [3]. The direct effect of these countermeasures on IS misuse intention has been reported by D'Arcy, et al. [10] and by D'Arcy and Hovav [45]. Information security policy is defined as a "state of the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations" [4]. Organizations develop security policies to ensure the security of information assets. So if an organization's end-users are not eager or are unwilling to comply with security policies, then these efforts are useless [15]. Furthermore, the literature on information security policies shows a need for empirical studies on security compliance [15].

Studies show that awareness of ISPs will decrease the behavioral intention to misuse [10, 30]. Herath and Rao [15] found that if users perceive that their compliance has a positive effect on the organization, they are more likely to have a positive attitude toward the security policies. Security policy can be best utilized by making sure that users understand it and accept its necessary precautions [10].

Organizations develop different controls to manage and control systems misuse, and SETA programs are a form of security countermeasure that serves this function of educating users about the major benefits of security [46, 47]. The contention is that just awareness campaigns and education help modify certain behaviors such as illegal drunk driving and shoplifting [10], in the same vein ongoing SETA programs convey knowledge about threats in the organizational environment which should help reduce system abuse and promote compliance with the ISPs. They work by providing information about the appropriate use of IS as well as stating clearly the disciplinary actions taken by the firm, including policies and sanctions for violations. Such programs provide the necessary knowledge of enforcement activities and reveals threats to local systems and their vulnerability to attack [10, 47, 48]. According to Straub and Welke [47], the wisdom behind SETA programs is that it serves to "convince potential abusers that the company is serious about security and will not take intentional breaches of this security lightly".

Computer Monitoring has two basic uses: providing feedback and implementing control. The feedback function intends to monitor employees so as to provide them with necessary suggestions for improvement. Monitoring for control is aimed at employee observation in order to foster compliance with rules and regulations [49]. The two combined eventually will help employees perceive that using ISPs in practice, including undertaking related roles and responsibilities, is relatively easy. So to gain conformity with rules and regulations, organizations adopt computer monitoring [10, 49]and different techniques are used to achieve this, including security audit, tracking users' internet usage, and recording network activities [10]. Studies have found that computer monitoring leads to a decrease in information resource misuse [10].

4. Research Methodology

4.1 Item Development

An initial survey instrument was developed by identifying and creating appropriate measurements based on a comprehensive literature review. The survey instrument is based on constructs validated and tested in prior research [4, 10, 13-15, 31], standardized and adapted to the context of this study. According to Straub [50] using validated and tested items will improve the reliability of results. The constructs include intention to comply, PUOP, PEOU, users' awareness of general information security, technology awareness, subjective norm and users' awareness of ISPs, SETA programs, and computer monitoring. The survey instrument was refined based on the feedback obtained from information security faculty members in United States and Jordan as well as from a number of employees working at a variety of banks in Jordan. Based on the feedback, several items were reviewed and modified. The instrument also collected key demographic information including gender, age, education, years of experience, functional area of work, and average length of time using a computer during the day.

4.2 Data Collection

The subjects of the study are banks' employees from Jordan. Surveys were randomly distributed to 350 employees at different managerial levels at all banks' departments. The questionnaire was distributed and administered to the subjects in a paper format. The survey instrument was handed to the participants, and they were asked to complete and return it within a week. The identities of participants were kept confidential. As a screener, participants were asked about their awareness of the existence of the ISPs and about their fluency in the English language. Only those

participants that indicated some awareness with ISPs and those that were fluent in English were included in the survey study. In the end 205 employees from 4 different banks participated and successfully completed the questionnaire. In reference to the characteristics of the instrument, and based on [51], the sample size exceeds the number recommended for conducting a factor analysis [51].

Table 1 summarizes respondents' descriptive statistics. Of the 205 respondents in the final sample, 44% were female, 52% were in the 20-29 age range, 79% held a bachelor's degree, and 25% had 11-15 years of experience. The average length of computer usage was 10.5 years, and the average use of computer noted at work was 6.6 hours per day. Participants reported using different computer software such as spreadsheet, word processing, e-mail, programming languages, database applications and bank's special tailored software. The sample was quite evenly distributed in terms of the responsibilities of the respondents and in terms of the managerial level. The data collected represents a diverse employee population since it includes employees from local as well as international banks in Jordan.

5. Data Analysis and Results

Partial least square (PLS) analysis was used to analyze the research model. PLS was used for two reasons: first, it avoids the problems of inadmissible solutions and factor indeterminacy, second: it has minimal demands for sample size [52]. In order to assess the measurement quality of the eleven reflective scales, convergent validity, reliability, and discriminant validity were calculated. Table 2 summarizes the items constituting the research model. The results show the questionnaire items, as well as the mean, standard deviation, factor loading of each item, and composite reliability (CR). The distribution of all variables was analyzed, and it was found that all variables included in the model were normally distributed. The number of factors was set to 11, which are the number of constructs included in the model. All 11 factors accounted for 63.2% of the total variance.

To provide an adequate basis for proceeding to an empirical examination of adequacy for factor analysis at the overall level as well as for each variable, an inspection of the correlation matrix was done. This revealed that most of the correlations are significant at 0.01 level. Bartlett's test was used to assess the overall significance of the correlation matrix and found to be significant at the 0.0001 level. To assess the patterns between variables, the measure of sampling adequacy (MSA) was computed. The overall MSA value was 0.788 which is higher than the acceptable range (above 0.50) [53]. As for each variable, MSA values were also found to be higher than the acceptable threshold of 0.50 [53].

To measure convergent validity, factor analysis was performed using the principal component extraction method followed by orthogonal varimax rotation. Convergent validity captures how well the measurement items relate to the construct, and it is acceptable if factor loadings of each measurement item with the one construct it is related to is at 0.70 or higher, and each item loads significantly on its latent construct [54]. The unrotated component analysis factor matrix revealed that some of the items did not load highly on their hypothesized factor or on any other factors. Varimax rotation was performed based on this observation, and most of the items loaded well on their latent constructs. Items that had low factor loadings or those that cross loaded on other factors were removed from the analysis. Results from the final rotated factor pattern matrix indicate that all items loaded with significant t-values on their respective latent constructs and have loading values above 0.70. Therefore, all these reflective scales exhibit sound convergent validity [54]..

To confirm the scale reliability and internal consistency, composite reliability (CR) and average variance extracted (AVE) was examined. A scale is deemed to be reliable if it has CR above 0.70 and an AVE of more than 0.50 [55]. Table 2 shows that all the reflective scales were reliable. These items will be used in future studies for testing the proposed theoretical research model.

To establish discriminant validity, both the loading and cross loading matrix (Table 2) and the correlation matrix (Table 3) were examined. All measurement items should load more strongly on their respective construct than on other constructs, which were found to be less than 0.50 for all items [55]. Second, Table 3 shows that the square root of AVE of each construct is higher than the correlations between that construct and any other construct (inter-correlations) [52]. As shown in Table 2 and Table 3, 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.

6. Conclusions

In this study, we have presented a Security Awareness Model that underscores the user dimension in addressing ISP compliance issues. This user focus, along with consideration of ISPs as a system, is a novel approach as compared to extant theoretical frameworks such as GDT, PMT, TRA, and TPB,

among others. The model tries to explain user compliance behavior with ISPs in terms of perceived ease of use of ISPs, perceived usefulness of protection afforded by ISPs, and the user awareness of information security issues and countermeasures. It is posited that among different factors, information security awareness likely plays a major role in shaping user compliance behavior with ISPs.

This article, which is part of the larger research study, is primarily focused on reporting the development, and validation of an instrument that can be used to test the proposed theoretical model. Based on the data analysis conducted, all the constructs in the measurement model are found to be valid and reliable. The validation of the measurement model serves as a first step towards the testing of our theoretical model.

The theoretical model, once validated, will be useful for practitioners, especially senior management, in understanding the factors that influence knowledge workers to comply with ISPs. It will also help in providing concrete guidance to management on how to implement ISPs in their organizations, so as to increase user compliance by proving incentives encouraging positive behavior. Additionally, it can also help in designing better information security training and education programs. Overall, this can lead to decreased cost of security, which is the primary issue of concern.

We acknowledge the limitations that relate to this study. One of the research limitations is concerned with the administration of the questionnaire, given that the researchers were not able to conduct this administration first hand and thus respond immediately to any unforeseen hurdles. The questionnaire was administered by some of the researchers' professional peers. Another 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. Lastly, the data was collected in a cross-sectional manner, which might lead one to measure a correlation rather than a causation effect. A major limitation to measuring "intention" is that it is self-reported, and so some employees might not express their true intention for different reasons.

7. References

[1] R. Richardson. (2009, Dec. 10). *14th Annual CSI Computer Crime and Security Survey. Executive Summary*. Available: http://www.personal.utulsa.edu/~james-childress/cs5493/CSISurvey/CSISurvey2009.pdf

[2] S. Kraemer, P. Carayon, and J. Clem, "Human and organizational factors in computer and information security: Pathways to vulnerabilities," *Computers & Security,* vol. 28, pp. 509-520, 2009.

[3] D. Straub, "Effective IS security," *Information Systems Research,* vol. 1, pp. 255-276, 1990.

[4] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly,* vol. 34, pp. 523-548, 2010.

[5] K. Beznosov and O. Beznosova, "On the imbalance of the security problem space and its expected consequences," *Information Management & Computer Security,* vol. 15, pp. 420-431, 2007.

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

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

[8] S. R. Boss, L. J. Kirsch, I. Angermeier, R. A. Shingler, and R. W. Boss, "If someone is watching, Ill do what Im asked: mandatoriness, control, and information security," *European Journal of Information Systems,* vol. 18, pp. 151-164, 2009.

[9] P. Puhakainen and M. Siponen, "Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study," *MIS Quarterly,* vol. 34, pp. 757-778, 2010.

[10] J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach," *Information Systems Research,* vol. 20, pp. 79-98, 2009.

[11] R. S. Shaw, C. C. Chen, A. L. Harris, and H.-J. Huang, "The impact of information richness on information security awareness training effectiveness," *Computers & Education,* vol. 52, pp. 92-100, 2009.

[12] J. A. Valentine, "Enhancing the employee security awareness model," *Computer Fraud & Security,* vol. 2006, pp. 17-19, 2006.

[13] H.-S. Rhee, C. Kim, and Y. U. Ryu, "Self-efficacy in information security: Its influence on end users' information security practice behavior," *Computers & Security,* vol. 28, pp. 816-826, 2009.

[14] T. Dinev and Q. Hu, "The centrality of awareness in the formation of user behavioral intention toward protective information technologies," *Journal of the Association for Information Systems,* vol. 8, p. 23, 2007.

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

[16] M. Siponen and A. O. Vance, "Neutralization: New Insights into the Problem of Employee Systems Security Policy Violations," *MIS Quarterly,* vol. 34, pp. 487-502, 2010.

[17] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "User acceptance of computer technology: a comparison of two theoretical models," *Management science,* vol. 35, pp. 982-1003, 1989.

[18] I. Ajzen, "Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior1," *Journal of Applied Social Psychology,* vol. 32, pp. 665-683, 2002.

[19] P. Puhakainen, "A design theory for information security awareness," Ph.D. Dissertation, University of Oulu, Finland, 2006.

[20] A. Kankanhalli, H. H. Teo, B. C. Y. Tan, and K. K. Wei, "An integrative study of information systems security effectiveness," *International Journal of Information Management,* vol. 23, pp. 139-154, 2003.

[21] S. Pahnila, M. Siponen, and A. Mahmood, "Employees' Behavior towards IS Security Policy Compliance," in *40th Annual Hawaii International Conference on System Sciences, HICSS 2007.* , 2007, pp. 156b-156b.

[22] C. L. Anderson and R. Agarwal, "Practicing Safe Computing Special Issue Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly,* vol. 34, pp. 613-643, 2010.

[23] A. C. Johnston and M. Warkentin, "Fear Appeals and Information Security Behaviors: An Empirical Study," *Management Information Systems Quarterly,* vol. 34, pp. 549-566, 2010.

[24] C. Jones, "Utilizing the technology acceptance model to assess employee adoption of information systems security measures," D.B.A. dissertation, Nova Southeastern University, United States -- Florida, 2009.

[25] G. Greene and J. D'Arcy, "Assessing the Impact of Security Culture and the Employee-Organization Relationship in IS Security Compliance," in *Proceedings of the 5th Annual Symposium on Information Assurance*, New York, USA, 2010, pp. 42-49.

[26] M. Siponen, S. Pahnila, and M. A. Mahmood, "Compliance with Information Security Policies: An Empirical Investigation," *Computer,* vol. 43, pp. 64-71, 2010.

[27] F. D. Davis, "A technology acceptance model for empirically testing new end-user information systems: theory and results," Sloan School of Management, Massachusetts Institute of Technology, Cambridge, MA, 1986.

[28] B. McCarthy, "New Economics of Sociological Criminology," *Annual Review of Sociology,* vol. 28, pp. 417-443, 2002.

[29] R. Paternoster and S. Simpson, "Sanction threats and appeals to morality: Testing a rational choice model of corporate crime," *Law & Society Review,* vol. 30, pp. 549-583, 1996.

[30] J. D'Arcy and A. Hovav, "Does one size fit all? Examining the differential effects of IS security countermeasures," *Journal of Business Ethics,* vol. 89, pp. 59-71, 2009.

[31] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *Mis Quarterly,* vol. 13, pp. 319-340, 1989.

[32] I. Ajzen, *Attitudes, Personality, and Behavior*: Milton Keynes, England: Open University Press, 1988.

[33] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS Quarterly,* vol. 27, pp. 425-478, 2003.

[34] V. Venkatesh and F. D. Davis, "A theoretical extension of the technology acceptance model: Four longitudinal field studies," *Management science,* vol. 46, pp. 186-204, 2000.

[35] J. Hartwick and H. Barki, "Explaining the role of user participation in information system use," *Management science,* vol. 40, pp. 440-465, 1994.

[36] P. A. Pavlou and M. Fygenson, "Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior," *Management Information Systems Quarterly,* vol. 30, p. 8, 2006.

[37] R. Agarwal, V. Sambamurthy, and R. M. Stair, "Research Report: The Evolving Relationship Between General and Specific Computer Self-Efficacy--An Empirical Assessment," *Information Systems Research,* vol. 11, pp. 418-430, 2000.

[38] C.-S. Ong, J.-Y. Lai, and Y.-S. Wang, "Factors affecting engineers' acceptance of asynchronous e-learning systems in high-tech companies," *Information & Management,* vol. 41, pp. 795-804, 2004.

[39] D. Trafimow, P. Sheeran, M. Conner, and K. A. Finlay, "Evidence that perceived behavioural control is a multidimensional construct: Perceived control and perceived difficulty," *British Journal of Social Psychology,* vol. 41, pp. 101-121, 2002.

[40] G. S. Kim, S. B. Park, and J. Oh, "An examination of factors influencing consumer adoption of short message service (SMS)," *Psychology and Marketing,* vol. 25, pp. 769-786, 2008.

[41] D. L. Goodhue and D. Straub, "Security concerns of system users : A study of perceptions of the adequacy of security," *Information & Management,* vol. 20, pp. 13-27, 1991.

[42] M. Siponen, "A conceptual foundation for organizational information security awareness," *Information Management & Computer Security,* vol. 8, pp. 31-41, 2000.

[43] M. Fishbein, "A reasoned action approach to health promotion," *Medical Decision Making,* vol. 28, p. 834, 2008.

[44] I. Ajzen, *Attitudes, personality, and behavior*: Maidenhead, Berkshire, England; New York: Open University Press, 2005.

[45] J. D'Arcy and A. Hovav, "Deterring internal information systems misuse," *Communications of the ACM,* vol. 50, pp. 113-117, 2007.

[46] G. Dhillon, "Managing and controlling computer misuse," *Information Management & Computer Security,* vol. 7, pp. 171-175, 1999.

[47] D. Straub and R. J. Welke, "Coping with systems risk: security planning models for management decision making," *MIS Quarterly,* vol. 22, pp. 441-469, 1998.

[48] M. D. Wybo and D. Straub, "Protecting organizational information resources," *Information Resources Management Journal (IRMJ),* vol. 2, pp. 1-16, 1989.

[49] A. Urbaczewski and L. M. Jessup, "Does electronic monitoring of employee internet usage work?," *Communications of the ACM,* vol. 45, pp. 80-83, 2002.

[50] D. Straub, "Validating instruments in MIS research," *MIS Quarterly,* vol. 13, pp. 147-169, 1989.

[51] R. L. Gorsuch, *Factor analysis* Second ed. Hillsdale, NJ: Erlbaum: Psychology Press, 1983.

[52] C. Fornell and D. F. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research,* vol. 18, pp. 39-50, 1981.

[53] J. F. Hair, W. C. Black, B. J. Babin, R. E. Anderson, and R. L. Tatham, *Multivariate Data Analysis*, Sixth ed. Upper Saddle River, NJ: Pearson Prentic Hall, 2006.

[54] D. Gefen and D. Straub, "A practical guide to factorial validity using PLS-graph: Tutorial and annotated example," *Communications of the Association for Information Systems,* vol. 16, p. 5, 2005.

[55] D. Gefen, D. Straub, and M. C. Boudreau, "Structural equation modeling and regression: Guidelines for research practice," *Communications of the Association for Information Systems,* vol. 4, p. 7, 2000.

Appendix

Table 1. Descriptive statistics of respondents

	Item	Freq.	Percent
Gender	Male	114	55.6
	Female	91	44.4
Age	20-29 years	108	52.7
	30-39 years	76	37.1
	40-49 years	21	10.2
Education	Bachelor's Degree	163	79.5
	Master	39	19
	PhD	3	1.5
Experience	1-5	98	47.8
	6-10	46	22.4
	11-15	50	24.4
	16-20	9	4.4
	> 20	2	1.0

Table 3. Discriminant validity of measurement model

	1	2	3	4	5	6	7	8	9	10	11
1. ITC	**.91**										
2.PUOP	.42	**.87**									
3.PEOU	.12	.15	**.91**								
4.SE	-.25	.25	.35	**.87**							
5.CONT	.34	.24	.15	.30	**.86**						
6.GISA	.25	.15	.39	.45	.03	**.83**					
7.TA	.36	.36	.09	.30	.15	-.24	**.90**				
8.ISPA	-.41	-.06	.01	.12	-.08	-.12	.05	**.93**			
9.SETA	.12	.45	-.29	.14	-.10	-.36	.03	.21	**.92**		
10.CM	.28	.32	.31	.11	.06	-.28	.01	.12	.12	**.89**	
11.SN	.12	.52	.20	.29	.43	-.02	.22	.17	.24	.24	**.92**

Table 4. Acronyms

ISP	Information Security Policy
RCT	Rational Choice Theory
PMT	Protection-Motivation Theory
GDT	General Deterrence Theory
PEOU	Perceived Ease of Use
PEOP	Perceived Usefulness of Protection
TPB	Theory of Planned Behavior
PBC	Perceived Behavioral Control
SETA	security education, training and awareness program
TRA	Theory of Reasoned Action
TAM	Technology Acceptance Model
PU	Perceived Usefulness
SN	Subjective Norms
SAM	Security Acceptance Model
C, Cont	Controllability
SE	Self-efficacy
ISA	Information Security Awareness
ITC	Intention to Comply
SE	Self-efficacy
GISA	General Information Security Awareness
TA	Technology Awareness
ISPA	Information Security Policies Awareness
CM	Computer Monitoring

Table 2. Measures Items and Item Loading

Items	Dimension/Questions	Mean	STD	Loading
ITC **CR = 0.720** **AVE = 0.832**	I intend to comply with the requirements of the ISP of my organization	4.48	1.79	0.858
	I intend to protect information resources according to the requirements of the ISP of my organization	3.98	1.51	0.782
	I intend to protect technology resources according to the requirements of the ISP of my organization.	4.01	1.41	0.761
	I intend to carry out my responsibilities prescribed in the ISP of my organization when I use technology resources	4.70	1.57	0.726
PUOP **CR = 0.915** **AVE = 0.760**	Complying with my organization's ISP addresses my job-related security needs.	4.72	1.49	0.834
	Complying with my organization's ISP saves me time.	4.91	1.51	0.865
	Complying with my organization's ISP enables me to accomplish tasks more securely.	4.57	1.50	0.844
	Complying with my organization's ISP reduces unproductive activities.	4.82	1.55	0.869
	Complying with my organization's ISP enhances my effectiveness on the job.	4.84	1.50	0.850
	Complying with my organization's ISP improves the quality of the work I do.	4.92	1.54	0.842
	Complying with my organization's ISP improves my productivity.	4.84	1.61	0.844
	Complying with my organization's ISP makes it easier to do my job.	4.91	1.59	0.806
	Overall, I find complying with my organization's ISP useful in my job.	4.85	1.57	0.865
PEOU **CR = 0.889** **AVE = 0.828**	Compliance with the requirements of my organization's ISP requires a lot of mental effort.	4.16	1.84	0.818
	I find it easy to recover from errors encountered when complying with my organization's ISP.	4.35	1.88	0.865
	The compliance requirements of my organization's ISP are rigid and inflexible.	4.42	1.92	0.815
	I find it easy to comply with my organization's ISP.	4.52	1.77	0.853
	I find it hard to comply with the requirements of my organization's ISP.	4.44	1.92	0.866
SE **CR = 0.890** **AVE = 0757**	**Self-Efficacy (0.890)**			
	I have the necessary competencies to fulfill the requirements of the ISP.	4.84	1.95	0.723
	If I wanted to, I could easily comply with my organization's ISP on my own.	4.53	2.06	0.790
	I would be able to follow most of the ISP even if there was no one around to help me	4.84	2.09	0.865
CONT **CR = 0.750** **AVE = 0.740**	I have the resources to protect my organization's information and technology assets from potential threats	4.82	2.01	0.720
	Threats to information security in my work are under control.	5.48	1.75	0.865
	In general, technology used at my organization is advanced enough to prevent information security threat	4.93	1.74	0.861
GISA **CR = 0.789** **AVE = .689**	Overall, I am aware of the potential security threats and their negative consequences.	5.06	1.74	0.715
	I have sufficient knowledge about the cost of potential security problems.	4.57	1.67	0.752
	I understand the concerns regarding information security and the risks they pose in general.	5.25	1.78	0.891
TA **CR = 0.801** **AVE = 0.810**	**Technology Awareness**			
	I follow news and developments about the security related technologies.	4.33	1.78	0.865
	I discuss Internet security issues or anecdotes with friends and people around me.	4.36	1.63	0.772
ISPA **CR = 0.787** **AVE = 0.865**	I am aware that my organization has a formal policy that forbids employees from installing their own software on work computers.	4.38	1.97	0.736
	I am aware of my organization's specific guidelines that describe acceptable use of computer passwords	4.20	1.73	0.833
	I am aware that my organization has a formal policy that forbids employees from modifying computerized data in an unauthorized way.	3.79	1.74	0.936
	I understand the rules and regulations prescribed by my organization's ISP.	3.75	1.92	0.739
	I understand my responsibilities toward enhancing my organization's information system security as prescribed in the organization's ISP.	3.68	1.81	0.746
SETA **CR = 0.775** **AVE = 0.846**	I am aware that my organization provides training to help employees improve their awareness of computer and information security issues.	4.40	1.66	0.777
	I am aware that my organization provides employees with education on computer software copyright laws	4.40	1.74	0.711
	I am aware that employees in my organization are briefed on the consequences of modifying computerized data in an unauthorized way.	4.26	1.66	0.869
	I am aware that my organization educates employees on their computer security responsibilities.	4.09	1.84	0.860
	I am aware that my organization educates employees on their responsibilities for managing computer passwords	4.81	1.70	0.908
	I am aware that my organization educates employees on appropriate use of information technology resources (e.g. email).	4.88	1.7	0.853
CM **CR = 0.778** **AVE = 0.792**	I am aware that my organization monitors any modification or altering of computerized data by employees	4.83	1.69	0.880
	I am aware that employees' computing activities are monitored by my organization.	4.63	1.84	0.867
	I am aware that my organization monitors computing activities to ensure that employees are performing only explicitly authorized tasks.	4.68	1.78	0.737
	I am aware that my organization reviews logs of employees' computing activities on a regular basis.	4.56	1.63	0.739
	I am aware that my organization conducts periodic audits to detect the use of unauthorized software on its computers.	4.44	1.61	0.867
SN **CR = 0.773** **AVE = 0.846**	Upper level management thinks I should comply with the requirements of my organization's ISPs.	4.73	1.84	0.767
	My boss thinks that I should comply with the requirements of my organization's ISPs.	4.75	1.87	0.804
	My colleagues think that I should comply with the requirements of my organization's ISPs.	4.77	1.80	0.825
	The information security/technology department in my organization thinks that I should comply with the requirements of my organization's ISPs.	4.61	1.97	0.763