5-20-2011

Information Security Policy Compliance: A User Acceptance Perspective

Ahmad Al-Omari
Dakota State University, Aaal-omari8026@pluto.dsu.edu

Omar El-Gayar
Dakota State University, omar.el-gayar@dsu.edu

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

Information Security Policy Compliance: A User Acceptance Perspective

Ahmad Al-Omari
Dakota State University
Aaal-omari8026@pluto.dsu.edu

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

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

ABSTRACT

Compliance with information security policies (ISPs) is a key factor in reducing an organization's information security risks. As such, understanding employees' compliance behavior with ISPs is an important first step to leverage knowledge worker assets in efforts targeted toward reducing information security risks. This study adapts the Technology Acceptance Model (TAM) to examine users' behavioral intention to comply with ISPs. The impact of information security awareness on behavioral intentions to comply is also considered in the research model. This is a research in progress, and an instrument is being developed to conduct a survey study to gather data from employees in the banking sector in Jordan.

Keywords: Information security awareness, compliance, information security policy, technology acceptance model, behavioral issues of information security.

INTRODUCTION

Information security has become one of the most important concerns and challenges facing organizations and users today. Studies concentrate on the need to design effective security policies (Whitman, Townsend, & Aalberts, 2001), as well as to motivate human and organizational factors to enhance users' security awareness to comply with ISPs (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009). Information security policies (ISPs) must be designed to provide employees with guidelines on how to secure information resources while they use information systems (IS) in performing their jobs (Straub, 1990; Whitman, et al., 2001). Although the creation of comprehensive ISPs and guidelines is given high priority, compliance with these policies is still lacking. Therefore, identifying the factors that motivate employees' awareness to comply with an organization's ISPs is an important step.

Drawing on the Technology Acceptance Model (TAM) (Davis, Bagozzi, & Warshaw, 1989), we propose a Security Acceptance Model (SAM). In this model, employees' intention to comply with the organization's ISPs is influenced by Perceived Ease of Use (PEOU) of ISPs and Perceived Usefulness of Protection (PUOP) afforded through the use of ISPs. The role of self-efficacy (SE) and controllability (C), which are rooted in the Theory of Planned Behavior (TPB) (Ajzen, 2002), have also been considered.

The proposed model captures some of the questions left unanswered by the previous studies. Besides, it is the first to completely examine the role of information security awareness in enhancing employees' compliance with ISPs. Specifically, the study will try to answer the following questions:

1. What is the role of information security awareness in forming employees' behavior toward compliance with ISPs?
2. What are the employees' perceptions about their roles and responsibilities, as set in the ISPs, in safeguarding organization's information resources toward compliance with ISPs?
3. What are the employees' perceptions about the degree of difficulty in complying with ISPs?

The next section presents a brief review of the relevant literature and highlights this study's contributions. The third section presents the research model. The fourth section describes the research methodology, survey instrument, sample, and data collection method.

LITERATURE REVIEW

Employees' compliance with ISPs is an important concern for organizations to prevent and reduce information system resources misuse and abuse by insiders (Straub, 1990). Studies that investigate end-user behavior argue that employees willingly choose to misuse or abuse the system (Bulgurcu, Cavusoglu, & Benbasat, 2010). Most empirical studies applied deterrence theory as a way to reduce system's abuse and misuse. Straub, (1990) found that different preventive and deterrent

techniques were found to be effective to reduce system abuse. (Kankanhalli, Teo, Tan, & Wei, 2003) found that greater deterrent effort appears to contribute to better IS security effectiveness. Similarly, (Pahnila, Siponen, & Mahmood, 2007) found that sanctions do not have an effect on employees' intentions to comply with ISPs.

Other studies employed different theories. Drawing on TPB and Rational Choice Theory, Bulgurcu, et al. (2010), found that attitude, normative belief, and self-efficacy have a significant effect on employees' intention to comply with ISPs. Drawing on Protection Motivation Theory along with the Theory of Reasoned Action and TPB, Anderson & Agarwal (2010) found that home computer users' intentions to perform security-related behavior are influenced by a combination of cognitive, social, and psychological factors. Siponen & Vance (2010) found that neutralization is an excellent predictor of employees' intention to violate ISPs. Johnston & Warkentin (2010) found that fear appeal is a positive predictor of a user's behavioral intention to comply with recommended individual security acts. Based on the Theory of Planned Behavior (TPB) and TAM, (Dinev & Hu 2007) found that higher awareness leads to higher confidence in preventing negative technologies; and PU and PEOU have no significant effect on users' intention to use protective technologies. Jones (2009) found that PU and Subjective Norms are significant predictors of employees' behavioral intention to use security controls. D'Arcy, Hovav, & Galletta (2009) found that users' awareness of security controls has an impact on sanctions perceptions which in turn reduced IS misuse intentions. Bulgurcu, et al. (2010) found that information security awareness has a strong effect on an employee's attitude to comply with the ISPs.

Various behavioral theories have been employed to study employees' compliance intentions with ISPs or to prevent systems misuse. 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 as a system that employees must accept first, as (Davis, 1986) did with the ordeal of accepting the technology. To address this gap, this research aims to develop a Security Acceptance Model (SAM), analogous to the TAM, to understand how information security awareness will enhance employees' compliance with ISPs by enhancing the degree to which they believe that putting ISPs into practice and engaging in the corresponding roles and responsibilities are relatively effortless (PEOU), and that using these roles and responsibilities to safeguard the organization's information technology resources will help their job duties and performance (PUOP).

RESEARCH MODEL

Based on TAM developed by (Davis, et al., 1989), a Security Awareness Model (SAM) (Figure 1) is proposed, which will help explain employees' intention to comply with ISPs. This study will examine the effect of external variables, namely perceived security protection mechanisms (security policies, Security education, Training and Awareness (SETA) programs, and computer monitoring) proposed and tested by D'Arcy & Hovav (2009), D'Arcy, et al. (2009), and Straub, (1990), controllability (Dinev & Hu, 2007; Rhee, Kim, & Ryu, 2009), information security awareness (Bulgurcu, et al., 2010) and self-efficacy (Dinev & Hu, 2007; Workman, Bommer, & Straub, 2008), on PUOP and PEOU of ISPs. Information security awareness is posited to directly influence employees' perceived usefulness toward compliance with ISPs (Bulgurcu, et al., 2010). The original relations in the TAM model are posited to hold in the context of ISPs too; PEOU and PUOP of ISPs are postulated to impact behavioral intention to comply. Based on the model (SAM) a number of hypotheses are developed. Table 1 provides definitions of the SAM constructs in the model and their sources.

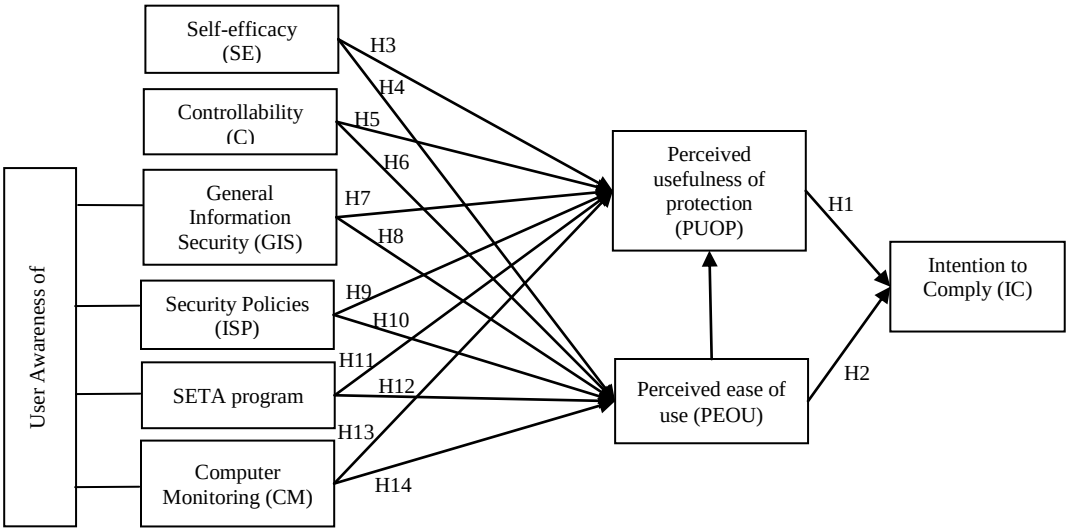

Figure 1: Research Model - Security Acceptance Model (SAM)

Table 1: Definitions and Sources of Constructs Taken from the Theory of Planned Behavior, and TAM

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)
Information security Policy (ISP)	State of the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations.	(Davis, 1989)
PUOP	The degree to which an employee believes that using ISPs' roles and responsibilities to safeguard the organization's information technology resources will enhance his/her job performance.	(Davis, 1989)
PEOU	The degree to which an employee believes that using ISPs' in practice and undertaking related roles and responsibilities is relatively easy.	(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)
Controllability	An individual judgment about the availability of resources and opportunities to perform the behavior.	(Bulgurcu, et al., 2010; Goodhue & Straub, 1991)
Information Security Awareness	An employee's overall knowledge and understanding of potential issues related to information security and their ramifications.	(D'Arcy, et al., 2009; Straub, 1990)
SETA programs	Passive security programs that are designed to deter misuse attempts by providing information regarding the proper use of information resources.	(D'Arcy, et al., 2009; Urbaczewski & Jessup, 2002)
Computer monitoring	Is an active security control that increases organization's ability to detect different IS resources misuse.	(D'Arcy, et al., 2009; Urbaczewski & Jessup, 2002)

In accordance with 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 his/her 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). The use of self-efficacy is consistent with the work of (Ajzen, 2002; Bulgurcu, et al., 2010; Fishbein & Cappella, 2006; Fishbein & Yzer, 2003). Controllability reflect the perceived ease of achieving an intended behavior (Ajzen, 1991), it is only, indirectly effect behavioral intention (Brown, Venkatesh, & Bala, 2006; Taylor & Todd, 1995). 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. An individual's awareness and knowledge of information security is built from life experiences or from external resources such as the Internet, newspapers, security journals (Bulgurcu, et al., 2010; Goodhue & Straub, 1991). As employees become more aware of information security, the more they perceived that using ISPs' in practice and undertaking related roles and responsibilities is relatively easy, and the more they believe that using ISPs' roles and responsibilities to safeguard the organization's information technology resources will enhance his/her job performance. Monitoring according to (Urbaczewski & Jessup, 2002) has two basic uses: providing feedback and implementing control. Monitoring for feedback is to monitor employees for providing them with necessary feedback and suggestions for improvement, while monitoring for control is to monitor employees in order to gain compliance with rules and regulations (Urbaczewski & Jessup, 2002). This eventually will help employees perceive that using ISPs' in practice and undertaking related roles and responsibilities is relatively easy.

CONCLUSIONS AND FUTURE WORK

We plan to conduct a survey study to investigate banks employees' perceived controllability, self-efficacy, and awareness of general information security, security policies, SETA program, and computer monitoring toward complying with the bank's ISPs to test the proposed security acceptance research model. A random sample of banks' employees in Jordan at different job levels and different departments will be taken. A sample of 10% of banks' employees will be taken in order to have 500 participants as a final sample that will have at least five times as many observations as the number of variables to be analyzed. The information will be collected directly by distributing the questionnaire to the banks' employees with help from a researchers' colleague who will supervise data collection.

Instruments for conducting the survey study are currently being designed. To ensure that the instrument is reliable and valid, the following procedures will be followed. To ensure content validity, in addition to drawing from published literature, the questionnaire will be given to a group of experts in the field, both in USA and Jordan, to verify that the content of the items are valid and measure what they are intended to measure. A pre-test will be conducted by distributing the questionnaire for a small group of employees, around 100; following up with a confirmatory factor analysis. Demographic information will be assessed in order to collect a sample that is very well matched demographically. Reliability test will also be conducted to measure the internal consistency for each construct.

In this article, we have proposed a new research model that can help understand the compliance behavior of employees with respect to ISPs. The research model is unique in taking a user acceptance perspective at this research issue. The conceptual research model and hypotheses are presented, and future work has been outlined.

References

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

Ajzen, I. (2002). Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior1. *Journal of Applied Social Psychology, 32*(4), 665-683. doi: 10.1111/j.1559-1816.2002.tb00236.x

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.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, Ill do what Im asked: mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164.

Brown, S. A., Venkatesh, V., & Bala, H. (2006). Household technology use: integrating household life cycle and the model of adoption of technology in households. *The Information Society, 22*(4), 205-218.

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.

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.

Davis, F. D. (1986). *A technology acceptance model for empirically testing new end-user information systems: theory and results.* Massachusetts Institute of Technology, Cambridge, MA. (Ph.D. Dissertation)

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *Mis Quarterly, 13*(3), 319-340.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management science, 35*(8), 982-1003.

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., & Cappella, J. N. (2006). The Role of Theory in Developing Effective Health Communications. *Journal of Communication, 56*(S1), S1-S17.

Fishbein, M., & Yzer, M. C. (2003). Using Theory to Design Effective Health Behavior Interventions. *Communication Theory, 13*(2), 164-183.

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

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

Jones, C. (2009). *Utilizing the technology acceptance model to assess employee adoption of information systems security measures.* D.B.A. dissertation, Nova Southeastern University, United States -- Florida. Retrieved from Dissertations & Theses: Full Text.(Publication No. AAT 3372768)

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.

Pahnila, S., Siponen, M., & Mahmood, A. (2007, Jan. 2007). *Employees' Behavior towards IS Security Policy Compliance.* Paper presented at the 40th Annual Hawaii International Conference on System Sciences, HICSS 2007. .

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.

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816-826.

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

Taylor, S., & Todd, P. (1995). Decomposition and crossover effects in the theory of planned behavior: A study of consumer adoption intentions. *International Journal of Research in Marketing, 12*(2), 137-155.

Urbaczewski, A., & Jessup, L. M. (2002). Does electronic monitoring of employee internet usage work? *Communications of the ACM, 45*(1), 80-83.

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.

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