Security Awareness and Security Training: An Attitudinal Perspective

Kamphol Wipawayangkool

The University of Texas at Arlington
Department of Information Systems and Operations Management, Arlington, Texas, 76019
Phone 817-272-3502, Fax 817-272-5801
kamphol.wipawayangkool@mavs.uta.edu

ABSTRACT

Although both researchers and practitioners recently acknowledge that managerial aspects of Information Security Management (ISM) finally arrive to the forefront of organizations, and that security awareness (SA) is crucial for successful ISM, behavioral aspects of SA have been not only inadequately studied but also lacking in theoretical justification. Two assumptions appearing in much of prior literature are either SA is considered a given independent variable or training is simply the key to SA improvement. To extend the relationship between security training and awareness, this paper, based on organizational behavior theory on job attitudes, proposes that overall job attitude moderates such relationship. Specifically, the propositions are developed: (1) security training is positively associated with improvement in SA, and (2) the extent to which security training is positively associated with improvement in SA is higher when overall job attitude is high. Both theoretical and practical implications are then discussed.

INTRODUCTION

Only recently have researchers and practitioners acknowledged that Information Security Management (ISM) is a multidimensional, not merely technical field as traditionally believed. This latest view emphasizes the significant interrelationship between individuals in organizations and the principles of ISM (Dhillon 2007; von Solms 2006). Recognizing that individuals are the key driver of operations within an organization, both researchers and practitioners agree that the weakest link in the ISM is not technology, but people. The consequences of malware threats are incomparable to those of human errors especially internal threats (Leach 2003). According to Computing Technology Industry Association (CompTIA), human errors account approximately 60% of security breaches in organizations in 2005, increasing from 47% in 2004 (Wagner 2006). Given the significance of people factors in ISM, two trends emerge in the literature. First, the focus has shifted from technical to managerial aspects of ISM. Indeed, researchers in behavioral paradigm analyze the security phenomena through individual-centric lens. As a result, unlike technical approach in which individuals often have to adapt to computer systems (hard approach), people approach (soft approach) does the opposite. Second, security policies and management at different levels in organizations such as strategic and operational, although extremely indispensable for any successful ISM, are often found to be ineffective because of the influences of variables such as individuals' motivation, attitude, commitment, norms, and other personal traits (Albrechtsen 2007; Jones 2007; Kruger and Kearney 2006; Leach 2003; Preining

1999; Ruighaver et al. 2007; Schweitzer 2005; Siponen 2000). Consequently, researchers suggest that building security awareness and culture is more effective than formalizing security policies alone (Ruighaver et al. 2007; von Solms and von Solms 2004; Vroom and von Solms 2004). In other words, the interest shifts from writing formal policies to applying those policies via building informal culture because of the impact of individuals' behaviors.

Emerging from this shift in paradigms, one of the recently highlighted dimensions in ISM is security awareness (SA) (Choi et al. 2006; Siponen 2000; von Solms 2001). Both researchers and practitioners have come to realize that SA is a fundamental yet critical factor for any successful ISM. Researchers suggest that investing in improving SA is more cost effective than that in advanced technologies (Jones 2007; Kelly 2006). Regardless of how advanced technologies are, the entire systems could fail if people neither are aware of the consequences of their actions nor behave as expected. Despite the significance of SA, several shortcomings in literature are present. First, the behavioral aspect of SA is currently understudied (Choi et al. 2006; Siponen 2000). Second, most SA studies have been done without much theoretical justification (Siponen 2000). Third, SA is often elaborated as a given independent variable in research models, while it is also critical to study how to improve SA, or consider SA as dependent variable. For example, Choi et al. (2006) examined the effects of security awareness and managerial actions on the ISM performance. Fourth, the effect of security training on awareness is often portrayed as simple relationship without considering the impacts of influential individual factors.

Given those shortcomings in literature, the objective of this paper is to extend the body of knowledge by (1) analyzing SA under behavioral lens by drawing from organizational theory on job attitudes, (2) focusing more on how to improve SA by placing SA as the dependent variable, and importantly, (3) presenting a more complicated relationship between security training and SA by including a significant individual factor, i.e. job attitude as a moderator. Collectively, the research question of this paper is: *Is there any effect of overall job attitude on the relationship between security training and security awareness improvement?*

This paper is organized as follows. First, the concept of SA and its significance in ISM are discussed. Second, the impact of security training on SA is discussed. Third, organizational behavior theory of job attitude and its role in developing the research model are discussed. Finally, both theoretical and practical implications are discussed.

LITERATURE BACKGROUND AND MODEL DEVELOPMENT

Security Awareness

According to the Information Security Forum (ISF) (2005), SA is defined as the extent to which organizational members understand the importance of information security, the level of security required by the organization and their individual security responsibilities, and act accordingly. Siponen (2000) defined SA as "a state where users in an organization are aware, ideally committed to, of their security mission". Dhillon (2007, p. 234) elaborated on SA such that "participants should be aware of the need for security of information systems and networks and what they can do to enhance security." This paper refers to the ISF definition because it includes not only the awareness state but also corresponding actions, which is arguably the more

important part (since actions may be able to justify whether individuals are aware of their actions). Nowadays, both researchers and practitioners acknowledge the significant role of SA. Von Solms and Von Solms (2004) considered people's SA one of the core importances in ISM. McCarthy, CEO of CompTIA, asserted that without users' security awareness, no technology on its own can be completely successful (Wagner 2006). Ernst & Young's 2004 Global Information Security Survey revealed that user awareness is the top obstacle (Johnson 2006).

SA is omnipresent in ISM principles. First, SA fundamentally exists in all dimensions of ISM (technical, formal, and informal management) (Dhillon 2007; von Solms 2006), indicating strong influence across all aspects. (Note that Dhillon classifies ISM into technical, formal, and informal aspects which are similar to von Solms' four waves.) Second, one of the key forces of the coming wave of security governance is SA (von Solms 2006). Regardless of the amount of capital invested in technical security and planning policy, the lack of either manager or user awareness will result in great risks (Straub and Welke 1998). Third, SA is the first principle needed to be considered for building strong IS security culture according to the Organization for Economic Cooperation and Development (OECD) (Dhillon 2007, p. 234). Thus, it may be appropriate to suggest that SA is an underlying culprit of the majority of unsuccessful ISM.

Despite its significance, SA is largely viewed as an independent variable in academic research, assuming that it exists as a given variable. Choi et al. (2006) studied the direct impact of managerial SA on organizational performance on ISM by assuming that SA is a given starting point in their model. Straub and Welke (1998), though stressing the underlying implications of SA, placed SA as one of their independent variables. In addition, the important yet elemental role of SA is insufficiently emphasized in research. Chang and Lin (2007) only explored the direct effect of organizational culture on ISM, while the model would have been richer if SA were included. SA has yet to offer more profound interpretations such as how to develop SA as ISM is now relevant more to people aspect than to IT. In sum, individuals need to be aware of and committed to their actions and the possible consequences in order to meet desired common goals of organizational ISM.

Security Awareness and Security Training

Many researchers and practitioners believe that security training is the key to improvement in SA. According to the Gartner Group, nothing in the security arena yields as much return on investment (ROI) as security training and awareness (Schultz 2004). Despite much investment in expensive advanced security systems, one could only imagine how much risk employees who naively handle sensitive information every day possess, if such information, which may be a source of competitive advantage of the firm, is transferred to competitors. All individuals must be trained how to handle information carefully according to the guidelines, and must be trained to become aware of the possible consequences of their actions. The major goal of security training is to mitigate risks (Johnson 2006). Risks can be either intentional or intentional. In this paper, the framework and discussion are more aligned with unintentional risks which are associated with the level of security awareness among individuals. Security training is an ongoing process as security policies evolve (Pabrai 2005). Some of the key topics for security training include motivating for better information security through regulations and rules, protecting the business through knowing how to handle information cautiously, and learning how

to recognize and avoid technical threats such as malicious software as well as practical ones such as security issues in physical settings (Pabrai 2005). Importantly, an assessment must be conducted to reinforce the learning outcomes from training (Pabrai 2005). An assessment should include questions to determine not only whether people understand and remember the knowledge, but also whether they apply it properly or comply with the policies (Johnson 2006).

Given the promising benefits of security training, it is definitely tempting to believe that providing training will simply lead to better awareness. Straub and Welke (1998) mentioned that in order to recognize security problems, security training should be provided to improve awareness. Johnson (2006) asserted that proper training and education help change people's mindsets and behaviors toward security. Bresz (2004) believed that without SA and training programs, people will always be the weakest link and organization will still be at risk. Kelly (2006) suggested that security training be required for all employees in order to improve awareness.

While the above views are absolutely legitimate, it is not complete. It is crucial not to lose sight of other influential factors that may play a role in the relationship between training and awareness such as employees' attitude, motivation, commitment, norms, and other individuals' characteristics (Albrechtsen 2007; Furnell 2006; Jones 2007; Kruger and Kearney 2006; Leach 2003; Preining 1999; Ruighaver et al. 2007; Schweitzer 2005; Siponen 2000). Schultz, the editor-in-chief of Computer & Security journal (2004), pointed out that determining the direct benefits of security training and awareness is much more challenging than it appears, and encouraged researchers to investigate such relationship in depth. For instance, Preining (1999) suggested that job satisfaction and commitment are important moral factors in order to improve users' SA. Furnell (2006) mentioned the lack of sense of community responsibility or commitment makes people ignore the possible consequences of their actions. Albrechtsen (2007) learned from their interviews with users that in addition to necessary knowledge, users do not perform security actions because of lack of motivation. Siponen (2000) discussed the delivery methods of security training and their effects on people's attitudes and motivation regarding how to raise the level of their SA. The training should rather increase people's insight on "how" and "why" than simply list what they should do. Traditional lecture approach is unlikely to improve people's attitudes and motivation.

This paper focuses on the paramount role of attitude. A change in attitude automatically leads to subsequent behavioral change (Nosworthy 2000). Other theories in IS research such as Technology Acceptance Model also embrace the explanatory power of attitude factor toward people's behaviors (Siponen 2000). Kruger and Kearney (2006) proposed a conceptual prototype for assessing SA through three specific dimensions: knowledge, attitude, and behavior. Their model views attitude as the key factor to determine what people think and act. Since the context of this paper revolves around the success of ISM which is based on employees as discussed, this paper investigates specifically overall job attitude rather than other aspects of attitudes. In the next section, this paper discusses the theory of job attitude and the development of the research model.

The Role of Job Attitudes

Job attitudes have long been studied in management literature. Job attitudes have been found to influence how trainees perceive their training experiences, how they react to the training (Sitzmann et al. 2008; Tannenbaum et al. 1991), and the evaluation or effectiveness of the training program (Mathieu and Martineau 1997, p. 205; Noe 1986; Sahinidis and Bouris 2008). Mathieu and Martineau (1997, p. 206) suggested that different attitudes are likely to affect training situations. One of the recent research models with strong prediction power ($r = 0.59$) is Harrison et al.'s attitude-engagement model (2006) which associates overall job attitude with individual effectiveness. Harrison and colleagues found that overall job attitude has considerable importance for understanding behavioral outcomes. In their model, job satisfaction and organizational commitment are the underlying dimensions of overall job attitude. Job satisfaction is defined as an emotional state resulting from the evaluation or appraisal of one's job experiences (Locke 1970). Organizational commitment is defined as a feeling of sharing beliefs and values with one's entire organization (Meyer and Allen 1991). Essentially, the attitude-engagement model states that "positive job attitude creates a tendency to engage or contribute desirable inputs to one's work role, rather than withhold them." Similarly, Sahinidis and Bouris (2008) found the significance correlation between employees' organizational commitment, job satisfaction, and motivation, and their perceived training effectiveness, which in turns will improves training outcomes.

Therefore, it is reasonable to apply Harrison et al.' attitude-engagement model to the research topic. That is, this paper extends the relationship between security training and awareness by integrating the moderating role of overall job attitude which is based on job satisfaction and organizational commitment. Specifically, employees with positive overall job attitude attending security training should be able to improve their security awareness in significantly greater extent than employees with negative overall job attitude. In the next section, the training outcome which is security awareness improvement in this paper is discussed.

Training Evaluation: Dimensions of Security Awareness

Recall the ISF definition of security awareness: the extent to which organizational members understand the importance of information security, the level of security required by the organization and their individual security responsibilities, and act accordingly. Clearly, two key dimensions of SA are to understand and to act.

Pointing that there is no theoretically based model of training evaluation and that mostly learning outcomes have been treated as uni-dimensional constructs, Kraiger et al. (1993) proposed the theory of learning outcomes. One of their assumptions is that learning outcomes are multidimensional, specifically cognitive, affective, and skill-based. To apply their classification, security awareness is viewed as a multidimensional learning outcome, which comprises cognitive and affective (understanding) and skill (acting). According to Kraiger et al. (1993), cognitive perspectives focus on both trainee knowledge, and the processes of knowledge acquisition, organization, and application. Stressing that attitudes can determine behavior or performance, Gagne (1984) originally defined affective based learning outcomes as internal state that influences the choice of personal action. Kraiger et al. (1993) expanded the definition to cover both attitudes and motivation by arguing that motivation is also internal state that affects behavior. Finally, skill-based learning outcomes involve two stages, namely compilation and

automaticity. Compilation occurs when trainee first builds smaller, discrete behaviors into a domain-specific routine, and then mentally combines steps by associating successive previously learned routines into a more complex behavior. Then, automaticity enables trainee to accomplish tasks without conscious monitoring. Collectively, a trainee attending security training is supposed to improve all dimensions of security awareness. Specifically, the trainee should learn all the principle of key knowledge about information security (cognitive), develop optimistic attitudes toward both specific content in training session and generic concepts of security (affect), and ultimately learn to act in secure manners (skills). From all the discussion above, the research model and propositions are developed as follows.

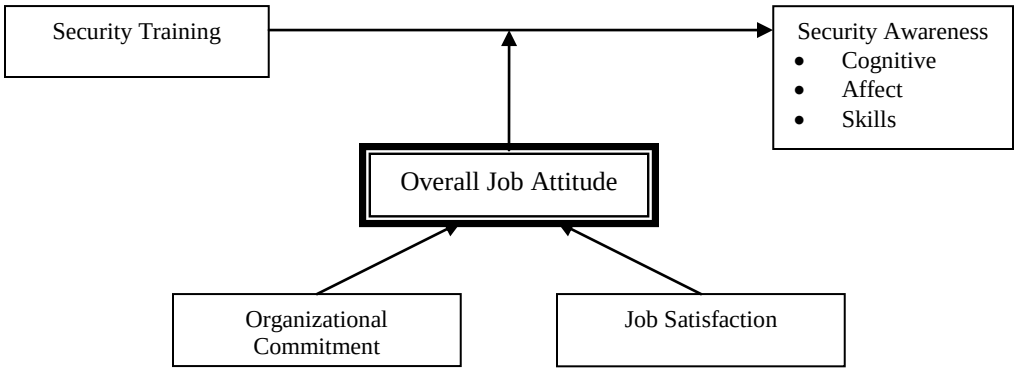

Figure 1: Research Model

Proposition 1. The security training is positively associated with improvement in security awareness (in all dimensions: cognitive, affect, and skill).

Proposition 2. The extent to which security training is positively associated with improvement in security awareness (in all dimensions: cognitive, affect, and skill) will be higher when overall job attitude is high.

IMPLICATIONS

Given the gaps in prior literature such as the understudied behavioral aspect of SA, the lack of theoretical justification, the assumption of SA as a given in the equation, and the simple relationship between SA and security training, this paper extends the body of knowledge of ISM, particularly of SA by analyzing SA under behavioral lens in more depth, drawing from an organizational theory on job attitude, not assuming SA as a given in the research model, and importantly offering a more complicated relationship between security training and SA by including a significant individual factor, i.e. job attitude as a moderator. In addition, I believe that the research model should pave the way for future researchers to investigate further the impacts of individuals' influential variables so that the simple relationship between SA and training can grow much richer. For practical implications, besides believing that security is another separate field or department in organization, managers should acknowledge that human resource department plays an important role such as ascertaining that employees are happily working with positive attitude toward their jobs and committed to the goals and objectives of organization. By including all these consideration, managers can be sure that the assigned

training will not go to waste simply because employees are not committed and have negative attitude toward their jobs.

REFERENCES

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, 26, 276-289.

Besnard, D., and Arief, B. (2004). Computer Security Impaired by Legitimate Users. *Computers & Security*, 23, 253-264.

Bresz, F.P. (2004). People—often the weakest link in security, but one of the best places to start. *Journal of Health Care Compliance*, 57-60.

Chang, S.E. and Ho, C.B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, 106, 3, 345-361.

Chang, S.E. and Lin, C. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems*, 107, 3, 438-458.

Choi, N., Kim, D.J., and Goo, J. (2006). Managerial Information Security Awareness' Impact on an Organization's Information Security Performance. *Proceedings of the Twelfth Americas Conference on Information Systems*, 3367-3375.

Dhillon, G. (2007). Principles of Information Systems Security: Text and Cases. John Wiley & Sons, Inc.

Furnell, S. (2006). Securing the home worker. *Network Security*, November, 6-12.

Hansche, S. (2001). Designing a Security Awareness Program: Part 1. *Information Systems Security*, January/February, 14-22.

Harrison, D.A., Newman, D.A., and Roth, P.L. (2006). How important are Job Attitudes? Meta-Analytic Comparisons of Integrative Behavioral Outcomes and Time Sequences. *Academy of Management Journal*, 49, 305-325.

Jahner, S. and Kremar, H. (2005). Beyond technical aspects of information security: Risk culture as a success factor for IT risk management. *Proceedings of the Eleventh Americas Conference on Information Systems*, 3327-3336.

Johnson, E.C. (2006). Security Awareness: Switch to a better programme. *Network Security*, February, 15-18.

Jones, D. (2007). Low Cost Security Tools: Employee Awareness. *Security*, November, 90-91.

Kelly, C.J. (2006). Awareness Trumps New Security Toys. *Computerworld*, October, 44.

Kotulic, A.G. and Clark, J.G. (2004). Why there aren't more information security research studies. *Information & Management*, 41, 597-607.

Kraiger, K., Ford, J.K., and Salas, E. (1993). Application of Cognitive, Skill-Based, and Affective Theories of Learning Outcomes to New Methods of Training Evaluation. *Journal of Applied Psychology*, 78, 2, 311-328.

Kruger, H.A., and Kearney, W.D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25, 289-296.

Leach, J. Improving user security behavior. *Computers & Security*, 22, 8, 685-692.

Mathieu, J.E., Martineau, J.W., (1997). Individual and Situational Influences on Training Motivation. In Ford, J.K, Kozlowski, S.W.J., Kraiger, K., Salas, E., and Teachout M.S (Eds.). Improving Training Effectiveness in Work Organizations (pp. 193-221). Lawrence Erlbaum Associates, Inc.

Meyer, J.P., and Allen, N.J. (1991). A Three-Component Conceptualization of Organization Commitment. *Human Resource Management Review*, 1, 1, 61-89.

Noe, R.A. (1986). Trainees' Attributes and Attitudes: Neglected Influences on Training Effectiveness. *Academy of Management Review*, 11, 4, 736-749.

Nosworthy, J.D. (2000). Implementing Information Security in the 21st Century – Do you have the balancing factors? *Computers & Security*, 19, 337-347.

Pabrai, U.O.A. (2005). Awareness Training: Strengthen Your Weakest Link. *Certification Magazine*, August, 28-29.

Preining, W. (1999). Prevention of information loss: An overview of what can happen and some simple guidance on how to prevent it. *Technology, Law, and Insurance*, 4, 13-22.

Ruighaver, A.B., Maynard, S.B., and Chang, S. (2007). Organizational security culture: Extending the end-user perspective. *Computers & Security*, 26, 56-62.

Sahinidis, A.G., and Bouris, J. (2008). Employee perceived training effectiveness relationship to employee attitudes. *Journal of European Industrial Training*, 32, 1, 63-76.

Schultz, E. (2004). Security training and awareness-fitting a square peg in a round hole. *Computers & Security*, 23, 1-2.
Schweitzer, D. (2005). Addressing the Human Security Vulnerability. *Computerworld*, October, 40.
Siponen, M.T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8, 1, 31-41.
Straub, D.W. and Welke, R.J. (1998). Coping With Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, December, 441-469.
Von Solms, B. (2001). Information Security – A Multidimensional Discipline. *Computer & Security*, 20, 504-508.
Von Solms, B. (2000). Information Security – The Third Wave? *Computers & Security*, 19, 615-620.
Von Solms, B. (2006). Information Security – The Fourth Wave. *Computers & Security*, 25, 165-168.
Von Solms, B and Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, 23, 371-376.
Von Solms, R and Von Solms, B. (2004). From policies to culture. *Computers & Security*, 23, 275-279.
Vroom, C., and von Solms, R. (2004). Towards information security behavioral compliance. *Computers & Security*, 23, 191-198.
Wagner, C.G (2006). Information Security's Biggest Enemy. *The Futurist*, July-August, 11.