Information Systems Security Training in Organizations: Andragogical Perspective

Research-in-Progress

Patrick I. Offor
Nova Southeastern University
po125@nova.edu

Gurvirender Tejay
Nova Southeastern University
tejay@nova.edu

Abstract

Organizations continue to suffer information systems (IS) security leaks, despite current research efforts by academia and practitioners to improve organizations' security compliance. IS security training has been identified as a major IS security threats mitigation strategy because personnel and administrative issues were recognized as major gaps between IS security threats and their countermeasures. Lack of employees' awareness has also been identified as a major obstacle to effective IS security posture. In addition, employee noncompliance with IS security policies and insider threats were acknowledged as fundamental security concerns for organizations. We argue that IS security awareness training and education are fundamentally important to an organization's ability to ensure policy compliance. Therefore, an effective IS security design and education, which are learner-centered, task-centered, problem-centered will be more relevant to an organization; hence, the adoption of Adult Learning Theory to examine the phenomenon.

Keywords

Information systems security, information security education, information security training, adult learning theory.

Introduction

Advances in information system (IS) security training design and education have lagged behind general systems development (Baskerville 1993), including security artifact, even though IS security training has been identified as a major IS security threat mitigation strategy. The lag is partly because of evolving threat signatures, treatment of IS security as afterthought in the project life cycle, and because personnel and administrative issues were recognized as major gaps between IS security threats and its countermeasures (Yeh and Chang 2007). Employee noncompliance with information systems security policies and IS security insider threats have been key concerns for organizations as well (Johnston and Warkentin 2010; Puhakainen and Siponen 2010; Stanton et al. 2005; Zeadally et al. 2012). The problem is that while an organization’s IS security training explicitly describes the impact of security leaks to the organization, it fails to explicitly explain the impact of such leaks to employees' wellbeing, except when it comes to personal identifiable information (PII) or protected health information (PHI). Obviously, technological advancement, especially in mobile computing, has heightened the importance of PII and privacy concerns (Cleveland 2012; Smith et al. 2011). The impasse is that organizations treat employees as an entity with the same level of experience in IS security context and with the same motivational silo. However, while older employee may be motivated to conform to organizations' IS security policies due to the security the job provides, younger employees may not. The misconception is the assumption that employees, regardless of their age, experience, and interest, are implicitly capable of deducing the importance of IS security compliance to organizations and to themselves. Lack of employees awareness has also been identified as a major obstacle to effective IS security posture (Rhee et al. 2012). In its report to congressional committees, the GAO Report (2011) identified information security program, which provides the framework for ensuring that IS security risks are understood, as one of the five common IS security weaknesses across its 24 agencies. Investments in nontechnical IS security mitigation measures yield nontangible benefits, as such; organizations find it difficult to quantify its actual value. Prior
research on IS security had focused on access control and on technology (Luo et. al. 2011; Chang et al. 2000). However, researchers have now refocused on people, an integral part of information systems, in order to identify the precursors to employees’ IS security policy behaviors and compliances in organizations upon the realization that effective management of secure information systems requires syndicated analysis of people, process, and technology (Hamill et al. 2005; Li et al. 2010). Equally noteworthy is that although IS security training is considered the most commonly suggested IS security compliance approach in literature, effectiveness of training design have not received the kind of academic exploration it deserves (Puhakainen and Siponen 2010). Literature review showed that there is a gap between IS security risks and control, due to employees’ IS security obliviousness, nonchalance, and no adherence to information systems security policies in organizations (Herath and Rao 2009; Spears and Barki 2010). Hence, the examination of effect of IS security training design and education based on andragogy, which focuses on adult learning (Knowles 1980: 43).

An effective IS security training that is learner-centered, task-centered, problem-centered will be more relevant, enhance knowledge acquisition, and improve organizational IS security compliance. IS security training must work as a compass to critically oriented knowledge (Closs and Antonello 2011). This is necessary since “education, training and awareness are perhaps the greatest non-technical measures available and a common theme for human factors and security” (Colwill 2010: 193). Furthermore, Hentea et al. (2006) argued for academic program to exploit and expose theoretical concepts and problem solving skills in IS security that is critical for jobs in organizations instead of relying solely on individual skills and certifications. Organizations take various IS security measures to improve their capabilities, their work systems, their people, and their development and implementation methods (Hevner et al. 2004); and securing organizations critical information systems is one way to ensuring a good return on investment. Dhillon and Torkzadeh (2006) found that maintaining IS security in organization requires adopting organizational grounded principles and values, in addition to technical considerations. To adopt such principles and communicate such values require greater efforts toward IS security design and education. Therefore, the belief is that identifying relevant precursors to training design, awareness, and compliance, as part of the holistic mitigation measures would help organizations secure their information systems.

We argue that IS security training design and education are fundamentally important to an organization’s ability to ensure information systems security policy compliance. This study examines how IS security awareness training design and education in organizations could be improved. This is necessary because safeguarding organizations’ critical information systems is economically, ethically, legally, and socially prudent in order to have “a well-informed sense of assurance that information risks and controls is in balance” (Anderson 2003: 310). Training design and education based on andragogy (Knowles 1980) should assess the conduciveness of training environment, the creation of platform that encourages participative planning and learning, the analysis of needs for learning, the design of IS security learning objectives, the development of learning activities, the media through which learning would occur, and the review and evaluation process.

**Literature Review**

Information systems security training design and education should have four elements: motivation, reinforcement, retention, and transference (Lieb 1991), which must work in concert to ensure that an effective training occurs. An effective training requires an effective training design. Therefore, one of the potency of our argument is that information systems training design must be in alignment with adult learning principles. The proposed alignment of the four elements identified above with the Adult Learning Theory—ALT (Knowles 1984) in Table 1, suggests that motivation provides the reasons for the IS security training and accounts for training participation due to internal and external pressures. Retention allows an individual to assimilate information in order to benefit from the training event as long as the individual is ready to learn, is oriented to learning, has reasons for learning, and has reservoir of knowledge upon which new knowledge is attached. Transference is the ability of an individual, in this context, in ensuring adherence to organization’s IS security policies, based on the individual’s capacity to make his or her own decision, and based on his or her understanding, relative to the person’s experience, about the risks and benefits of noncompliance. Reinforcement sustains individual behaviors that are in conformity with organizations’ IS security policies, and discourages those that are not. Nonetheless, the objective, from ALT prism is to ensure that individuals’ training experiences are relevant to their positions and the
responsibilities they hold, and that training lead them to their assigned tasks. Most studies in information security had focused on one or more of the elements described above. However, this study is aimed at examining the four components in unison using ALT theoretical framework and show that effective information security training design and education must motivate employees, activate retentiveness, encourage unconscious desire to adhere to information security policies and reinforce positive behavior.

Review of literature revealed that effective IS security education will help in activating employees’ thinking process (Puhakainen and Siponen 2010) and in internalizing the significance of compliance. Hence, the extrapolation is that a well-designed IS security education would create IS security awareness by stimulating employees’ sensitivity to personal and organizational vulnerabilities and threats. The second conviction is that effective training design will equip employees with the necessary IS security skills and inspire adherence to IS security policies in the performance of their assigned and implied tasks (NSTISSI 1994). Adults have a broader base of experience on which to attach new ideas and skills (Knowles 2005); focusing on training design that aims at providing reasons for and benefits of training rather than just checking-the-block (Davis and Davis 1990) will better information systems security training. In addition, tailoring of IS security education will provide employees with richer meaning and better reasons for IS security compliance in organizations. Employees are motivated to learn (Davis and Davis 1990) and to act (Herath and Rao 2009) intrinsically and extrinsically; their satisfaction with IS security training will nourish and motivate them and will ultimately improve their IS security awareness and compliance.

**Motivation as Element of Learning**

Dweck (1986) found that motivational process influences the way individuals deploy their existing skills and knowledge, how they acquire new ones, and the effectiveness of transference. It is motivation that
drives or stimulates an individual to sign up for graduate studies, stay the course, and achieve academic excellence. Motivation drives, inspires, and sustains behaviors in many ways, whether it is for a positive behavior or a negative one. From andragogy and from IS security stand point, a training design that allows an employ to understand exactly why certain precautions must be taken to safeguard organization’s critical information systems will prepare the employee better to receive the training. There are two types of motivations: intrinsic and extrinsic motivation (Herath and Rao 2009; Brekke et al. 2003; Murdock 2002; Siponen 2000). Siponen (2000) described intrinsic motivation as act of self-determination in which an individual or a group justifies their actions based on internal reasons and their own aspirations. In other words, the initiation and the sustained drive to an action is based on internal pressure; for example, self-desire to do the right thing, complete an assignment, conform to organizations’ IS security policies. Conversely, extrinsic motivation deals with the application of pressure to act based on external pressure i.e., compliance to security policy due to peer-pressures, fear of penalty, or the severity of penalty. Despite the differences between intrinsic and extrinsic motivation, Herath and Rao (2009) suggests, “Security behaviors can be influenced by both intrinsic and extrinsic motivators.” Puhakainen and Siponen (2010) described several how users’ compliance actions were dictated, in part by external motivators.

**Retention**

Employees’ ability to conform to an organization’s information systems security policies depend, in part, on the employees understanding of what is required from him or her. Hence, IS security design and education must provide an employee with the reasons why he or she must comply with organization’s IS security policies. The misconception is that we usually have unrealistic expectation, consequently, we negates the fact that we are also product of our environment and that adults have divers background and knowledge and come from all works of life. Secondly, there is a need for IS security training to be in alignment with an employee’s position or responsibilities within an organization, or the types information systems available to the employee. In addition, IS security training design and education must be employee centered, which means that the training must lead employees to tasks upon which they about to undertake. In other words, the training must be relevant to sustain users’ attention and must be useful to users in the performance of their job. Lieb (1991) suggested that a learner must see a meaning or purpose in order to retain information being taught. Drevin et al. (2007) indicated that periodic assessment of staff member’s IS communication and technology is necessary, hence our position is that assessment of employees’ IS security awareness is necessary, since employee errors are among the top threats to IS security. Information systems security training design and education currently require transformational learning—premise reflection, obtainable only through critical reflection and reflective discourse (Merriam 2004). Premise reflection allows us to reflect on our held experiences, belief, values, feelings, or dispositions (Merriam 2004). We must also design training and education in such a way that compels learners to reflect on their actual work and training experiences—content reflection, and how to protect themselves and the organization from security threats—process reflections.

**Transference**

Lieb (1991) described transference as the ability of a learner to use the information garnered in a course in a new setting. In IS security context, training design and education considerations should include design and training efforts that are geared toward the ease of transference, in order to encourage users to retain and transfer what they have learned in the classroom or on the web to their workplace, so as to protect critical information systems in their organizations. This is important because adults believe in their personal capacities to making their own decisions and expect others to see their capacities to self-directions according to Knowles (1984). There are two types of transference: positive and negative. A positive transference is preferred because it is a situation in which employees apply what they have learned in an IS security training, whereas negative transference is the opposite.

**Reinforcement**

Information training design and education should consider incorporating reinforcement initiatives during the initial training design planning. In other words, addition of reinforcement activities during IS security training design should not be an afterthought. Although positive and negative reinforcements are geared toward desired outcome, they are different in that positive reinforcement encourages and sustain good behaviors, whereas negative reinforcement discourages undesired behaviors. This is necessary because
empirically, employees wish for good outcome for themselves and others, as well as for their organization (Herath and Rao 2009). In Herath and Rao (2009), negative reinforcement, penalty and certainty of detection proved to be a reinforcement tool, but severity of penalty did not exert any significant influence on security behavior intentions. Bulgurcu et al. (2010) illustrated the impact of using sanctions (tangible and intangible penalties, such as demotions, reprimand, unfavorable action, or monetary penalties) as reinforcement as well.

**Theoretical Framework**

Information systems security threats and vulnerabilities in organizations are diverse, dynamic, and evolutionary, thus, assessing influencers to resultant training needs are valid and prudent propositions. For example, in acquisitions logistics, initial and sustainment training and education are integral to a product lifecycle, without which effective employment of the product over its lifecycle may be shortened or derailed; likewise, effective IS security awareness training design and education should be a continuous exercise in information system security management. Closs and Antonello (2011: 64-65) argued, “Management education [training] should provoke a transformation of the thinking mode, allowing managers to integrate the economic, ethic, politic, social, and environmental dimensions involved in their work, all at same time.” It is important that organizational information systems security awareness training provide employees among other things, reasons for taking appropriate IS security policy actions that protect organizations’ business interest as well as employees’ personal interest, since empirical and anecdotal evidences suggest that there is a need for organizations to stay ahead of their employees’ security behaviors. Table 2 is a composite alignment and description of IS security constructs derived from Adult learning theory principles.

**Perceived Value**

In the context, perceived value is the value learners attribute to new knowledge or skill they acquire. Adults want to know how what they are learning applies or improves their real life situations or improves their job performances or quality of life. Perceived value may also be described as the perceived net benefits (Kim and Kankanhalli 2009). This means that a typical adult learner wants to know if what he or she is learning is valuable and how the knowledge is going to bridge the gap between where he or she is now in terms of knowledge and where he or she wants to be. Therefore, on the presumption that employees are more likely to lend themselves to learning when they understand the essence of the training and its value to organizations and to themselves, we postulate that employees perceived value has a causal relationship with employees’ IS security training design and education.

**Informal Learning**

Mocker and Spear (1982) lifelong learning model was broken into four parts: formal learning (learner has no control learning objectives or means of the learning); nonformal learning (learner controls the objectives, but not the means); informal learning (learner controls the means, but not the objectives); and self-directed learning (learner controls both the objectives and the means). One assumption in andragogy is that adults believe in their personal capacity to making their own decision and expect others to see their capacity to self-direction. Lowry (1989) stated that an estimated 70% of adults learning is self-directed learning by taking learning initiative with or without other people’s help. In addition, anecdotal evidence shows the importance and the practicality of informal learning in organization. Therefore, we predict that informal learning, which allows organizations to maintain control of their IS security training objectives, but allows employees the flexibility to choose the means of learning, will signify acceptance of employees’ capacity to self-concept and will significantly influence their IS security training and awareness.

**Self-Identity**

Adults have diverse experiences and they self-identify with who they are and what they have done (Knowles 2005). Adult learners are more heterogeneous in terms of their background, learning style, need, motivation, interest, and goals. The contention is that IS security training design and education that exploit employees’ experiences would make the training an enhancing event. Enhancing events are events that are consistent with individual self-identity, and threatening events are those that are inconsistent.
Since individuals tend to engage in enhancing events and avoid threatening events (Guo et al. 2011), the goal of IS security education would be for employees to keep IS security in mind as they deal with organizations’ vital information systems daily (Whitman 2003). Consequently, the prediction is that employees who self-identify with their organizations’ IS security training, would respond positively to organizations’ awareness training and would respond better to their organization’s IS security requirements.

Table 2. Adult Learning Theory Assumptions and Information Systems Security

<table>
<thead>
<tr>
<th>Adult Learning Theory (ALT) Concepts</th>
<th>Description of the Concepts</th>
<th>IS Security Construct</th>
<th>Description of the Constructs</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Need to know</td>
<td>Adults have a need to know why and how the learning applies to real life situation.</td>
<td>Perceived Value</td>
<td>This deals with learners’ perception of how the learning will improve their performance or quality of life.</td>
<td>(Dhillon and Torkzadeh 2006; Knowles 1980)</td>
</tr>
<tr>
<td>Learner’s self-concept</td>
<td>Adults believe in their personal capacities to making their own decisions and expect others to see their capacities to self-directions.</td>
<td>Informal Learning</td>
<td>Organizations or institutions need to have control of their IS security training objectives, but employees or learners may need to have the option to choose the delivery method, i.e., classroom, Web training, hybrid etc.</td>
<td>(Mocker and Spear 1982; Lowry, 1989)</td>
</tr>
<tr>
<td>Role of experience</td>
<td>Adults have wealth of experiences—they self-identify with who they are and what they have done.</td>
<td>Self-Identity</td>
<td>Individuals tend to engage in enhancing events and avoid threatening events.</td>
<td>(Guo et al. 2011; Knowles 1980)</td>
</tr>
<tr>
<td>Readiness to learn</td>
<td>Learning experience should coincide with associative developmental tasks—a task that arises at certain stage of a person’s employment.</td>
<td>Responsibility based Learning Experience</td>
<td>IS security type training should be tied to the type of information systems available or would immediately become available to the employee at a time, based on their position or level of responsibility.</td>
<td>(Knowles 1980; Havighurst 1972)</td>
</tr>
<tr>
<td>Orientation to learning</td>
<td>Adults orientation to learning are life-centeredness, task-centeredness, or problem-centeredness.</td>
<td>Timing of Employee-centered instruction</td>
<td>IS security training events should be aligned to lead employees to their assigned and implied tasks.</td>
<td>(Jonassen 1999; Knowles 1980)</td>
</tr>
<tr>
<td>Motivation</td>
<td>Adults, unlike young people, are motivated intrinsically more with job satisfaction, self-esteem, and quality of life.</td>
<td>Intrinsic Pressure</td>
<td>Adult learners respond to both intrinsic and extrinsic motivations. Therefore, information security context, adults intrinsically and extrinsically motivated.</td>
<td>(Herath and Rao 2009; Knowles 1980)</td>
</tr>
<tr>
<td></td>
<td>Adults are also extrinsically motivated with promise of better jobs, higher salaries and the like.</td>
<td>Extrinsic Pressure</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Responsibility Based Learning Experience

Adult learners learn those things that help them work better in their workplace and in their real-life situation. It is important that learning experience is associative with developmental task. For example, in an academic setting, teaching a freshman a graduate level course may not be helpful to the student at that point in time and may be a turn off. Likewise, tailoring IS security training to employees' functional need in the organization will serve the individual and the organization better. A “developmental task is a task which arises at or about a certain period of life of the individual, successful achievement of which leads to the person’s happiness and to success with later tasks, while failure leads to unhappiness in the individual, disapproval by the society, and difficulty with later tasks” (Havighurst 1972). IS security training should be tied to tasks relating to the use of information systems.

Timing of Employee-Centered Instruction

Adults’ orientation to learning is life-centered or task-centered or problem-centered (Knowles et al. 2005). Learners orient training to real life applications. Which means that employees would be motivated to participate in IS security awareness training, to the extent that such awareness training would help them perform their job better or deal with their life situations. Objectivist learning assumes that knowledge is transferred from the instructor to the learner, or acquired by the learner. Conversely, constructivist assumes that “knowledge is individually constructed and socially co-constructed by learners based on their interpretations of experiences in the world” (Jonassen 1999: 217). The suggestion is that adult learning leans toward constructivism; i.e., focusing on employees because of their large reservoir of experiences will help individuals to self-identify with the organization’s security education. Therefore, we predict that timing of IS securing training event or learning experience to developmental tasks will positively affect organizations IS security training and awareness.

Motivation as a Construct

Adults respond to intrinsic pressures (job satisfaction, self-esteem, and quality of life) as well as to extrinsic pressures (better job, promotion, and higher salary). Based on andragogy and in IS security-training context, the prediction is intrinsic and extrinsic pressures would have casual effect on organizations’ IS security training design and education as suggested in Herath and Rao (2009). Therefore, although the study is more interest in intrinsic motivation because adults are motivated more internally (Knowles 1990), we will evaluate the role of extrinsic motivation as well because adult are also motivated externally, especially when dealing with new knowledge acquisition.

Implication of the Study

The outcome of this study will show that IS security awareness training design and education based on Adult Learning Theory would enhance employees’ IS security awareness and compliance in organizations by incorporating four training elements: motivation, reinforcement, retention, and transference throughout IS security training design. The notion is that such consideration and application of the elements as described would allow for transformational learning through premise reflection. This is necessary because “failure to identify and implement mitigation measures against security threats and vulnerabilities have exponential implications” (Offor 2013: 478) and costs. The study will confirm or disconfirm Adult Learning Theory in the context of IS security training design and education. In addition, the study will show that organizations can improve their information security posture by developing IS security training that explicitly explains the essence of IS security compliance to the organizations as well as to the employees. Time and again, organization are so bent on informing their employees about the implication of noncompliance to the organization and they forget to explain to the employees how their jobs and general wellbeing depend also on the effectiveness of collective management of critical information systems assets in the organization. Finally, pursuant to a more comprehensive and better IS security mitigation measures, the study will advanced our understanding of ALT and its relationship to information system security management in organizations.
Conclusion

The crèche is that employees should be well rehearsed over time with an organization’s information systems practices and would need only periodic sustainment training. For all intents and purposes, periodic training will reinforce IS security behaviors in so far as the training is relevant to current IS security threats and vulnerabilities. Secondly, many organizations do not report their security leaks and attacks; as such, some employees may think that information systems security warnings are phantasm. Furthermore, current training designs focuses mainly on the importance of IS security compliance to organizations and explain the implications explicitly, yet leave employees to infer the importance of the threats to self implicitly. Information systems security design and education should inculcate in employees, the threat to themselves and others, as well as the threat to the organization. Adult learners are more heterogeneous in terms of their background, experience, learning style, need, motivation, interest, and goals. Therefore, IS security education should be problem-centered, task-centered, and employee-centered.

References


