Exploring the Effect of Knowledge Transfer Practices on User Compliance to IS Security Practices

Tonia San Nicolas-Rocca, San Jose State University, San Jose, CA, USA
Benjamin Schooley, University of South Carolina, Columbia, SC, USA
Janine L. Spears, DePaul University, Chicago, IL, USA

ABSTRACT

Institutions of higher education capture, store and disseminate information that is protected by state and federal regulations. As a result, IS security policies are developed and implemented to ensure end user compliance. This case study investigates end user knowledge of their university’s IS security policy and proposes a new approach to improve end user compliance. The results of this study suggest that users may be contributors to the transfer of IS security policies when provided with an opportunity to participate in the development of an IS security awareness and training program.

Keywords: Case Study, Compliance, Higher Education, IS, IS Security

1. INTRODUCTION

Institutions of higher education collect, store and disseminate information that is protected by state and federal regulations including the Family Education Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), and Protections of Pupil Rights Amendment (PPRA). In response, higher education organizations are tasked with guiding their institutions in the quest to safeguard data, information systems, and networks; protect the privacy of the higher education community; and ensure that information security is an integral part of campus activities and business processes (Grajek, 2013).

The development and implementation of an information systems (IS) security policy is a mechanism used by institutions of higher education to guide business processes, organizational tasks and activities, and to ensure compliance

DOI: 10.4018/ijkm.2014040105
to state and federal laws and regulations. It has been reported extensively that employees, also known as insiders, do not comply with IS security policies (Bulgurcu et al., 2010; Johnson and Warkentin, 2010; Myyry et al., 2009; Vance and Siponen, 2012; Straub, 1990; Willison and Warkentin, 2013). If users do not comply, institutions of higher education could be at serious risk of regulatory liabilities and lawsuits (Myyry et al., 2009; San Nicolas-Rocca and Olfman, 2013; Warkentin et al., 2011).

IS security continues to be a managerial concern, and has been identified as one of the top challenges facing institutions of higher education (Grajek, 2013). According to Privacy Rights Clearing House (2013), approximately 200 institutions of higher education reported data breaches between 2010 and April, 2013. Of these incidents, approximately 80 were due to end user activity, including the unintended disclosure of and/or an insider’s explicit intent to share sensitive information.

In other reports, users have directly or indirectly caused over half of all reported security breaches (Dhillon and Moores, 2001). Insider threat continues to be a significant challenge, captures a great deal of public attention (Willison and Warkentin, 2013; Shaw and Stock, 2011), and methods to improve compliance are needed.

To improve compliance, organizations have relied on IS security education, training and awareness (SETA) programs. Although it is widely accepted that these programs are important for maintaining the effectiveness of information security and privacy techniques and procedures for user compliance (Warkentin et al., 2011; Shaw and Stock, 2011), it is also important to recognize that many of these programs have been considered useless (Karjalainen and Siponen, 2011) or have been found ineffective (Albrechtsen, 2007).

The success of SETA programs depends on the ability of the training facilitator to engage trainees (Cone et al., 2007). When the instructor is able to effectively communicate the applicability and practical purpose of the material to be mastered, as distinguished from abstract or conceptual learning, the learning retention rates and the subsequent transference of the new knowledge or skill to the trainees is enhanced (NIST SP 800-16, 1998). For IS security programs aimed at user compliance, this essentially means that the training method can affect the transference of knowledge to trainees, which can therefore influence the effectiveness of IS security training and awareness programs.

The theory of knowledge transfer has been discussed in the IS literature (Alavi and Leidner, 2001; Nonaka, 1994). Several factors have been identified as having an influence on knowledge transfer in the implementation of information systems (Ko et al., 2005). These include absorptive capacity, motivation, and communication (Alavi and Leidner, 2001; Ko et al., 2005). However, empirical results regarding the effects of knowledge transfer in IS security training or awareness for user compliance have not been reported. Furthermore, addressing knowledge transfer in IS security training and awareness for user compliance where the user is not only trained, but actively participates in the development of an IS security program has not been reported. This study addresses these gaps by focusing on user training and participation in the development of an IS security program within higher education to improve end user compliance.

This paper provides the final results and discussion of this research project. Preliminary findings reported in this article were presented at a conference in early 2014 (San Nicolas-Rocca et al, 2014). The remainder of this paper proceeds as follows. First, a review of knowledge transfer, and user participation in information systems development is covered. We then describe the research location and method used. This is followed by a discussion of the findings, and implications for practice and research.

2. LITERATURE REVIEW

2.1. Knowledge Transfer

Knowledge is taken to be transferred when learning takes place and when the recipient
Related Content

NLS: A Reflection Support System for Increased Inter-Regional Security
[www.igi-global.com/article/nls/117868?camid=4v1a](www.igi-global.com/article/nls/117868?camid=4v1a)

The Role of Creativity, Innovation, and Invention in Knowledge Management
[www.igi-global.com/chapter/role-creativity-innovation-invention-knowledge/68328?camid=4v1a](www.igi-global.com/chapter/role-creativity-innovation-invention-knowledge/68328?camid=4v1a)

Managing Complex Adaptive Social Systems
[www.igi-global.com/chapter/managing-complex-adaptive-social-systems/49049?camid=4v1a](www.igi-global.com/chapter/managing-complex-adaptive-social-systems/49049?camid=4v1a)
Online Knowledge Sharing Among Chinese and American Employees: Explore the Influence of National Cultural Differences

Wei Li (2009). *International Journal of Knowledge Management* (pp. 54-72).

[www.igi-global.com/article/online-knowledge-sharing-among-chinese/4053?camid=4v1a](www.igi-global.com/article/online-knowledge-sharing-among-chinese/4053?camid=4v1a)