Engaging Remote Employees: The Moderating Role of “Remote” Status in Determining Employee Information Security Policy Awareness

Allen C. Johnston, School of Business, University of Alabama at Birmingham, Birmingham, AL, USA

Barbara Wech, School of Business, University of Alabama at Birmingham, Birmingham, AL, USA

Eric Jack, School of Business, University of Alabama at Birmingham, Birmingham, AL, USA

ABSTRACT

Using social cognitive theory as a framework, this study proposes and tests a behavioral model to predict how “remote” status impacts the manner in which social learning cues influence employee awareness of information security policies and ultimately differentiates him or her from in-house employees in terms of information security policy awareness. Based on data acquired from an online sample of 435 full-time employees across numerous industries and structural equation modeling analysis, the findings suggest that, compared to their in-house counterparts, remote employees experience lower levels of vicarious experiences, verbal persuasion, and situational support, thereby resulting in diminished levels of information security policy awareness. These findings have strong implications for managers of remote employees and for organizations seeking to reduce the risk associated with an ever-increasing remote workforce. The findings also advance social cognitive theory by incorporating information security policy awareness as an important outcome formed from perceptions of social learning cues external to the individual, but present within the organization.

Keywords: Awareness, Information Security, Policy, Remote Employee, Social Cognitive Theory

INTRODUCTION

Organizations are constantly pushing out the perimeter of their organizations to encompass a variety of stakeholders, including partner firms, clients, or branch office employees. A significant driving force for this network expansion is the emergence of social networks and mobile applications and the new business practices that result from Web 2.0 based opportunities. As part of this shift, organizations are becoming increasingly reliant upon a mobile workforce (Barsness, Diekmann, & Seidel 2006), whereby employees are no longer co-located in a shared organizational setting, but are geographically and, perhaps, temporally dispersed (Staples, Hulland, & Higgins, 1999). Defined as non-managerial employees that spend at least 50% of their work hours away from the confines of

DOI: 10.4018/joeuc.2013010101
a corporate office, remote employees represent an understudied but growing class of employee (Goldsen, 2006). Recent reports highlight this growth trend, documenting that remote or virtual workforces are growing rapidly, increasing from 12.4 million telecommuters in 2006 to 17.2 million in 2008 (Foster, 2009). In fact, Forrester Research predicts that by 2016, 43% of U.S. workers will telecommute to some extent.

As the information technologies (IT) that support remote workers continue to evolve, the reliance upon the traditional, centralized model for employee workspaces is lessened. Further, the advances in IT have made it easier for organizations to embrace remote employment options among their workforce. For both remote and internally housed employees (in-house employees), the ability to access and transmit information from resources maintained within the organization is critical to their success. With such access, however, comes the threat of exposing sensitive systems and information to threats, both internal and external (Loch, Straub, & Kamel, 2003; Png & Wang, 2009). Results from a 2010 PricewaterhouseCoopers survey of security professionals from over 500 organizations worldwide indicates that both the number of attacks on information resources and the financial cost of such incidents have increased significantly over 2008 levels, with the direct and indirect cost associated with external attacks increasing threefold since 2008 (Potter & Beard, 2010). The survey report also indicated that staff are increasingly involved as both a victim and as an unwitting accomplice to the attackers, with 46% of the survey respondents reporting a loss or leak of confidential data due to poorly trained or improperly monitored staff.

How employees respond to behavioral controls is determined in part by social learning cues that exist within the environment in which they work (Bandura, 1977; Gist & Mitchell, 1992). Also referred to as workplace environmental stimuli or intra-organizational pressures, social learning cues represent forces that exist outside of the employee but within the organizational setting in which the employee operates. For remote users, telecommuters, or employees that travel frequently, the social learning cues are perhaps less obvious in that many of the reinforcement activities and mechanisms in place within the firm to distribute policies and other behavioral controls are not present at home, in vehicles, or in remote offices (hotels, etc.) (Lewis, Agarwal, & Sambamurthy 2003; Wiesenfeld, RaghuRam, & Garud, 1999; Liang & Xue, 2010). For these individuals, many of the external persuasive social forces that influence policy awareness are simply not prevalent in their remote workplaces. As a result, remote employees may be less aware or informed about information security policies and the associated procedures for providing a reasonable level of protection to information assets.

While numerous studies have examined the antecedents of policy compliance among employees (Johnston & Warkentin, 2010b, 2010a; Smith, Milberg, & Burke, 1996; Warkentin & Willison, 2009; Willison & Siponen, 2009), the vast majority of these studies have focused on compliance struggles among in-house employees and the behavioral controls that influence their compliance perceptions, intentions, and behaviors. For instance, Tyler and Blader (2005) compare the efficacy of extrinsically and intrinsically-oriented strategies for promoting policy compliance. However, their study sample of 540 respondents from a large multinational financial services company does not distinguish between in-house or remote employees. Warkentin, Johnston, and Shropshire (2011) also do not distinguish between in-house and remote employees in their examination of the informal social learning environment on information privacy policy compliance intent. As a final example, Aytes and Connolly (2004) examine a rational choice model for understanding user behavior toward policies, yet consistent with the extant literature, also do not differentiate in-house users from remote users in their study. Clearly, there exists a gap in the literature and our subsequent understanding of the role of remote status in determining outcomes relative to information security policy compliance.

Further, few studies have examined the influential factors that lead to information
Ergonomic User Interface Design in Computerized Medical Equipment
[www.igi-global.com/chapter/ergonomic-user-interface-design-in-computerized/18200?camid=4v1a](www.igi-global.com/chapter/ergonomic-user-interface-design-in-computerized/18200?camid=4v1a)

Pervasive or Invasive? A Strategic Approach to IT-Enabled Access and Immediacy
[www.igi-global.com/article/pervasive-invasive-strategic-approach-enabled/37220?camid=4v1a](www.igi-global.com/article/pervasive-invasive-strategic-approach-enabled/37220?camid=4v1a)