What Drives Information Security Policy Violations among Banking Employees?
Insights from Neutralization and Social Exchange Theory

Pei-Lee Teh, Monash University, Bandar Sunway, Malaysia

Pervaiz K. Ahmed, Monash University, Bandar Sunway, Malaysia

John D'Arcy, University of Delaware, Newark, DE, USA

ABSTRACT

Employees' information security policy (ISP) violations are a major problem that plagues organizations worldwide, particularly in the banking/financial sector. Research shows that employees use neutralization techniques to rationalize their ISP violating behaviors; it is therefore important to understand what leads to and influences these neutralization techniques. The authors' study draws upon social exchange theory to develop a set of factors that drive employees' neutralization of ISP violations. The model specifies previously untested relationships between job satisfaction, organizational commitment, role conflict, role ambiguity, and neutralization techniques. Using a sample of Malaysian banking employees, the authors found a positive relationship between role conflict and neutralization of ISP violations, whereas organizational commitment was negatively related to neutralization in this context. The authors' findings offer fresh insights for scholars and practitioners in dealing with the problem of employees' intentional ISP violations while extending the reach of neutralization theory beyond North American and European cultures.

Keywords: *Information Security, Job Satisfaction, Neutralization Theory, Organizational Commitment, Role Conflict, Role Ambiguity, Social Exchange Theory*

INTRODUCTION

Information systems (IS) security is a major challenge for businesses across the globe. Banking and financial institutions, the subject of the current study, are particularly vulnerable to IS security threats. PricewaterhouseCoopers recently published its Global Economic Crime Survey involving 3877 respondents across 78 countries, and reported that 45 percent of financial organizations suffered information-related fraud in the prior 12 months compared to 30

DOI: 10.4018/jgim.2015010103

percent in other sectors (PricewaterhouseCoopers, 2013). Being information intensive organizations, banking institutions have historically needed to develop and maintain effective control systems in order to prevent IS security breaches. Despite these efforts, a recent survey indicated that 94 percent of banks were affected by employee-related breaches (Department for Business Innovation & Skills, 2013). This finding is consistent with the views of IS security scholars (Warkentin & Willison, 2009), who contend that employees' non-compliance with information security policies (ISP) is a major security concern. In fact, evidence suggests that over half of all IS security breaches stem from employees' lack of policy compliance (Wilson, 2009).

The IS security literature provides various definitions and meanings to describe ISPs. In the technical literature, the term "policy" is synonymous with the security architecture of operating systems; hence, an ISP describes access control rules for a computer system (Baskerville & Siponen, 2002). There are also executive-level ISPs, which articulate senior management's overall security strategy and vision for the organization (Whitman, 2007). And at the operational level, an ISP can be described as "a statement of the roles and responsibilities of the employees to safeguard the information and technology resources of the organization" (Bulgurcu, Cavusoglu, & Benbasat, 2010, pp. 526-527). Operational-level ISPs describe what employees should and should not do with organizational IS resources and include a set of formalized policies, procedures, and technical controls to which employees are required to adhere (i.e., acceptable usage guidelines). Consistent with several earlier IS studies (e.g., D'Arcy, Hovav, & Galletta, 2009; Siponen & Vance, 2010), we consider ISPs in this manner for the current study.

In our context, an ISP violation is therefore any act by an employee that is against the established operational-level ISP of the organization. Although some employees bypass these ISPs with harmful intentions, such as stealing sensitive corporate data or computer sabotage, evidence suggests that most deliberate ISP violations are not overtly malicious (Wilson, 2009). Recent categorizations of internal IS security threats use the term *volitional (but not malicious) noncompliance* to classify such actions (Guo, Yuan, Archer, & Connelly, 2011). Common violations of this sort include leaving a computer logged on when away from the desk, sharing passwords with a co-worker, writing down passwords, copying confidential company data to unapproved portable devices (e.g., unencrypted USB drives), and sharing sensitive information with non-employees (Stanton, Stam, Mastrangelo, & Jolten, 2005). Each of these activities puts the organization's data at risk for leaks and breaches and has been linked to more extreme security breaches (Verizon Business Systems, 2010). Moreover, these types of ISP violations are particularly salient in the banking and financial industries, where protection of organizational information assets is of utmost concern.

There is growing body of academic literature aimed at explaining employees' compliance/noncompliance with ISPs. Several theories of Criminology and Psychology have been applied in this regard, including: Neutralization Theory (Siponen & Vance, 2010; Siponen, Vance, & Willison, 2012), Deterrence Theory (D'Arcy et al., 2009; Herath & Rao, 2009), Rational Choice Theory (Li, Zhang, & Sarathy, 2010), the Theory of Planned Behavior (Bulgurcu et al., 2010), Protection Motivation Theory (Siponen, Mahmood, & Pahnila, 2014), and the Theory of Cognitive Moral Development (Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009), to name a few. Sommestad, Hallberg, Lundholm, and Bengtsson (2014) provide a systematic review of this body of work. Although these theory-driven studies provide substantive insight into employees' ISP violations and related behaviors, our knowledge of the phenomenon remains incomplete. To this point, Willison and Warkentin (2013) recently advocated three topics for future behavioral IS security research: neutralization techniques, expressive or instrumental criminal motivations, and employee disgruntlement. In the current

Related Content

On-Line User Interaction with Electronic Catalogs: Language Preferences Among Global Users

Aryya Gangopadhyay and Zhensen Huang (2000). *Journal of Global Information Management (pp. 16-23).*

www.igi-global.com/article/line-user-interaction-electronic-catalogs/3541?camid=4v1a

Impact of Mobile and Wireless Technologies on Developing Countries

Ran Neuman (2008). *Global Information Technologies: Concepts, Methodologies, Tools, and Applications (pp. 988-1000).*

www.igi-global.com/chapter/impact-mobile-wireless-technologies-developing/19021?camid=4v1a