A Composite Framework for Behavioral Compliance with Information Security Policies

Salvatore Aurigemma, Communication and Information Sciences (CIS) PhD Program, University of Hawaii at Manoa, Honolulu, HI, USA

ABSTRACT

To combat potential security threats, organizations rely upon information security policies to guide employee actions. Unfortunately, employee violations of such policies are common and costly enough that users are often considered the weakest link in information security. This paper presents a composite theoretical framework for understanding employee behavioral compliance with organizational information security policies. Building off of the theory of planned behavior, a composite model is presented that incorporates the strengths of previous studies while minimizing theoretical gaps present in other behavioral compliance models. In building the framework, related operational constructs are examined and normalized to allow better comparison of past studies and help focus future research efforts.

Keywords: Information Security, Information Security Policies, Information Systems, Security, Security Threats

INTRODUCTION

Information systems are pervasive throughout the spectrum of modern international organizations including the education, military, government and commercial sectors. Worldwide spending on information technologies and services by the year 2014 is estimated to be $4 trillion (Hardcastle et al., 2012). Unfortunately, with the increased reliance of the U.S. economy on information and information systems come increased information security threats and associated costs. Information security concerns are not isolated to the U.S.; information security compromises occur internationally on a daily basis with losses potentially in the range of hundreds of billions a year (United Nations, 2005).

Capturing the true cost and occurrence of information security incidents is a difficult task. It is estimated that organizations only discover a fraction of actual security incidents (Whitman, 2003). Additionally, many organizations are reluctant to admit security breaches due to a variety of reasons, such as negative publicity or reputation damage (Richardson, 2011; Hoffer & Straub, 1989; Panko, 2009). This information dilemma is not limited to small organizations with limited information security resources.

DOI: 10.4018/joeuc.2013070103
Since 2010, RSA Inc., Verisign Inc. (both companies at the forefront of digital encryption and security technology), and Google were hacked by what is now being called Advanced Persistent Threats (APTs) (Andress, 2011; Reeder, 2012). APTs are defined as a technologically sophisticated entity engaged in information warfare (use of IT to gain an advantage over an adversary) in support of long-term goals (Cloppert, 2009). While the damage done to RSA and Google was primarily conducted by complex computer software remotely operated via computer networks, it was human error that opened the organizations to attack. Specifically, the recent successful APT attacks against RSA Inc. and Internet giant Google both started with spear-phishing attacks that successfully tricked employees to open email attachments that included unknown software vulnerabilities (Andress, 2012).

The importance of employees on information security. There are numerous threats to the confidentiality, integrity, and availability of organizational information and information systems (Panko, 2009). While there are many security mechanisms designed to mitigate the information security risks from relevant threats, it is often incumbent upon users to utilize the technologies and/or procedures faithfully and properly for them to be effective; information security depends on the effective behavior of humans (Siponen, 2005; Stanton et al., 2005; Vroom & von Solms, 2004; Workman, 2007; Panko, 2009). In a report by the U.S. National Security Telecommunications and Information Systems Security Committee (NSTISSC), the greatest potential threat to government information resources is said to come from “insiders with legitimate access to those systems” (NSTISSAM, 1999).

There is ample and important research on the information security dangers of organizational insiders. There are generally two types of insider security risks – those from malicious and non-malicious employees (NSTISSAM, 1999; Brackney & Anderson, 2004). In the well-respected 2010/2011 Computer Security Institute (CSI) Computer Crime and Security Survey, over 60% of respondents reported losses due to security compromises from non-malicious insiders, compared to 41% from malicious insiders (Richardson, 2011).

To assist users in ensuring information security during the use of information technologies and resources, organizations provide employees information security policies (ISPs) (Panko, 2009; Ernst & Young, 2011). An ISP describes employee roles and responsibilities, addressing specific security issues, in protecting the information resources of their organization (Panko, 2009; Bulgurcu et al., 2010). Unfortunately, occurrences of employee non-compliance with the guidance provided in their ISPs is significant (Stanton et al., 2005), resulting in billions of dollars annually in losses to their organizations (Calluzzo & Cante, 2004). It is for this reason that employees are often considered the weakest link in information security (Mitnick et al., 2002; Warkentin & Willison, 2009; Zhang et al., 2009).

Given the importance of the employee in information security, it is essential to identify and better understand the determinants of security behavior. Behavioral compliance research findings can help focus organizational efforts toward improving employee compliance with ISPs (Zhang et al., 2009; Herath & Rao, 2009; Workman et al., 2008; Ng et al., 2009; Bulgurcu et al., 2010; D’arcy et al., 2009; John & Warkentin, 2010; Guo et al., 2011). The challenge for organizations is to know how to transform users from the biggest information security vulnerability to the first line of ISP compliance defense (Straub & Welke, 1998; Ng et al., 2009). In order to address this challenge, research is required on employee security behavior and on methods to enhance employee compliance.

Significant empirical research effort has been expended, particularly in the past five years, towards obtaining a better understanding of the factors affecting employee behavioral intent to comply with ISPs. A review of the literature shows some commonalities in the supporting theories used in related research. However, the varied conceptual implementations of these theories have resulted in a confusing array of behavioral compliance models and
Diffusing Management Information for Legal Compliance: The Role of the IS Organization within the Sarbanes-Oxley Act
[www.igi-global.com/chapter/diffusing-management-information-legal-compliance/38088?camid=4v1a](www.igi-global.com/chapter/diffusing-management-information-legal-compliance/38088?camid=4v1a)

User Behaving Badly: Phenomena and Paradoxes from an Investigation into Information System Misfit
[www.igi-global.com/chapter/user-behaving-badly/18213?camid=4v1a](www.igi-global.com/chapter/user-behaving-badly/18213?camid=4v1a)

Are Information Systems’ Success and Failure Factors Related? An Exploratory Study
[www.igi-global.com/chapter/information-systems-success-failure-factors/18182?camid=4v1a](www.igi-global.com/chapter/information-systems-success-failure-factors/18182?camid=4v1a)