Information Resources Management Journal
Volume 31 • Issue 1 • January-March 2018

Roles of Organizational Climate, Social Bonds, and Perceptions of Security Threats on IS Security Policy Compliance Intentions

Princely Ifinedo, Department of Financial and Information Management, Cape Breton University, Sydney, Nova Scotia, Canada

ABSTRACT

The objective of this study was to investigate employees' information systems security policy (ISSP) compliance behavioral intentions. Theoretical frameworks, including the Theory of Planned Behavior, the Social Bond Theory, and Organizational Climate (OC) perspective were integrated to facilitate this process. A survey of working professionals in Canada was conducted. Relevant hypotheses were formulated and data analysis was performed with the partial least square structural equation modeling technique. The results show that OC contributes indirectly to ISSP compliance intentions via the social bonding constructs, but does not have a direct effect on ISSP compliance. Of the social bonding constructs, only commitment was found not to be related to ISSP compliance intentions. OC influences employees' perceptions of IS security threats and attitudes toward compliance, which in turn impacts ISSP compliance intentions. Additionally, employees' perceptions of IS security threats have an insignificant effect on ISSP compliance intentions, but indirectly impact compliance via attitude and personal norms. The contributions and implications of the study for practice and research are highlighted

INTRODUCTION

Information systems (IS) have become a key resource to organizations because such assets are used to realize strategic intent and are critical in ensuring an organization's long-term survival (Arvidsson et al., 2014). A breach of an organization's IS assets can cause dire financial losses and serious non-financial problems (Bulgurcu et al., 2010; Hu et al., 2011; UK BIS/PWC, 2014; PricewaterhouseCoopers, 2014; Bauer and Bernroider, 2017). A survey in the United Kingdom reported that the average annual cost of information security breaches in large organizations was between £600,000 (USD $920,000) and £1.15 (USD $1.76) million (UK BIS/PWC, 2014). A global estimate of the cost of information security breaches to both small and large organizations runs in the billions of dollars (Ponemon Institute, 2014). Accordingly, the protection and safety of IS resources has become a major concern to organizations across the world (Bulgurcu et al., 2010; Guo et al., 2011; Ifinedo, 2015; Ponemon Institute, 2016; Han et al., 2017; Bauer and Bernroider, 2017).

Justifiably, attention has shifted toward IS security control and management (Ashenden, 2008; Zhao and Xue, 2009; Kolkowska et al., 2017) in an effort to protect and safeguard valuable IS-related assets. More often than not, organizations tend to rely on technology-based solutions to contain risks to their IS assets (Bulgurcu et al., 2010). However, the reality is different as evidence suggests that organizations that neglect the roles of individuals are less successful in their efforts to achieve desired outcomes (Stanton et al., 2005; Guo and Yuan, 2012; Crossler et al., 2013; Safa et al., 2016; Kolkowska et al., 2017) because technology-based approaches can only go so far. Furthermore, huge financial investments committed to technology-based security solutions have not resulted in

DOI: 10.4018/IRMJ.2018010103

decreased IS security risks and threats (Öğütçü et al., 2016). Experts argue that achieving success with IS security means prioritizing both technology-based solutions and human-related factors (Vroom and von Solms, 2004; Ng et al., 2009; Furnell and Clarke, 2012; Crossler et al., 2013; Kolkowska et al., 2017). The focus of this study will be on the latter since technical-related aspects of IS security management have been previously researched (e.g., Zafar and Clark, 2009).

The human agent (i.e., an organization's employees) is considered the weakest link in the chain of effective IS security management and control (Crossler et al., 2013; Ifinedo, 2014). In fact, the insider (i.e., employees) is viewed as a serious threat to organizations' IS resources (Boss et al., 2009; Symantec Corporation, 2014; PricewaterhouseCoopers, 2015). A recent report showed that current employees cause more than 50 percent of security breaches in their organizations (PricewaterhouseCoopers, 2015). Another trade report indicated that executives believe the actions of a company's own employees pose more immediate danger than external threats (CITI, 2015). In brief, the behavior of the insider often facilitates breaches to an organization's IS assets (Lowry and Moody, 2015). For example, employees who download unauthorized software or visit illicit websites that may contain malicious code may inadvertently allow unscrupulous outsiders to harm their organization's IS resources.

One tool commonly used to control insider security behaviors is the information systems security policy (ISSP), which encompasses ethical computer use policies, acceptable use policies, email use policies, and social media use policies, among others. ISSPs may be explicitly formalized or implicitly stated within other organizational rules and procedures (Bulgurcu et al., 2010; Son, 2011; Ifinedo, 2012). Regardless, such tools spell out the guidelines and procedures employees must follow in order to safeguard an organization's IS resources and the consequences of policy violations (Lowry and Moody, 2015; Yazdanmehr and Wang, 2016). However, the availability of an ISSP does not guarantee that employees will adhere to its stipulations. This is because employees either intentionally or unintentionally flout such rules for a multitude of reasons, including ignorance, complacency, negligence, apathy, mischief, and resistance (Siponen and Vance, 2010; Herath and Rao, 2009a; Lowry and Moody, 2015; Siponen et al., 2014; Safa et al., 2016; Stafford, 2017). The study by Hinde (2002) suggested that up to 91% of workers in organizations do not comply with their ISSPs. Indeed, employee noncompliance of ISSPs poses a serious IS security problem in practice (Siponen and Vance, 2013; Symantec Corporation, 2014, PricewaterhouseCoopers, 2015). Admittedly, the effectiveness of an ISSP and related rules hinges on employee compliance (Crossler et al., 2013; Son, 2011). According to Yazdanmehr and Wang (2016), "without employees' compliance, an [ISSP] cannot serve as an effective countermeasure to information security problems" (p.36).

Against this backdrop, research on how to motivate employees to comply with ISSPs has received – and continues to receive – a lot of researchers' attention (Pahnila et al., 2007; Herath and Rao, 2009a, 2009b; Boss et al., 2009; Bulgurcu et al., 2010; Siponen and Vance, 2010; 2014; Son, 2011; Vance et al., 2012; Ifinedo, 2012; Chen et al., 2012; Ifinedo, 2014; Siponen et al., 2014; Yazdanmehr and Wang, 2016; Safa et al., 2016; Bauer and Bernroider, 2017; Han et al., 2017; Kolkowska et al., 2017). The systematic review of ISSP compliance literature (Sommestad et al., 2014; Lebek et al., 2014; Alaskar et al., 2015) indicated that research in the area has benefitted mainly from behavioral and criminological theories. While knowledge of ISSP compliance is advanced by such prior efforts, it is important to accept that compliance, being a complex concept, should be studied from differing perspectives to further enhance knowledge (Ifinedo, 2014). Researchers (e.g., Vroom and von Solms, 2004; Stanton et al., 2005; Pahnila et al., 2007; Bulgurcu et al., 2010) have also argued that a broad range of perspectives, including socio-organizational and human-related factors, need to be duly considered.

This study draws from the Theory of Planned Behavior (TPB) (Ajzen, 1991), which past research revealed is the most widely used theoretical framework for studying ISSP compliance (Sommestad et al., 2014; Lebek et al., 2014; Alaskar et al., 2015). It is worth mentioning that TPB was chosen because it is axiomatic among scholars across disciplines that theory can explain innumerable behaviors, including ISSP compliance (Armitage and Conner, 2001; Lebek et al., 2014). In order to diversify