Computers in Human Behavior 68 (2017) 190–209

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Full length article

Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals

A.J. Burns [a, *], Clay Posey [b], Tom L. Roberts [a], Paul Benjamin Lowry [c]

[a] Department of Computer Science, College of Business and Technology, The University of Texas at Tyler, 3900 University Blvd., Tyler, TX 75799, USA
[b] Department of Information Systems, Statistics, and Management Science, Culverhouse College of Commerce, The University of Alabama, USA
[c] Faculty of Business and Economics, The University of Hong Kong, Hong Kong, China

ARTICLE INFO

Article history:
Received 30 March 2016
Received in revised form
31 October 2016
Accepted 12 November 2016

Keywords:
Information security
Psychological capital (PsyCap)
Protection motivation theory (PMT)
Positive psychology
Organizational insiders

ABSTRACT

Practitioners and researchers alike recognize the positive influence insiders' behavior can have on information systems (IS) security. This awareness has resulted in a research stream focused on the performance of protective behaviors. We contribute to this research stream by extending an oft-cited theory in the information security literature—protection motivation theory (PMT)—to include the relationship of insiders' psychological capital (PsyCap) with the mechanisms of PMT.

PsyCap is a construct of role-breadth psychological capacities and resources embodying important work-related motivational resources. Therefore, given the varied facets central to PMT, determining the relationship of PsyCap with each distinct PMT mechanism is an important contribution. Furthermore, prior research has established that individuals can develop their PsyCap. Consequently, considering the relationship of role-breadth PsyCap with the PMT mechanisms provides an important and malleable, motivational antecedent that complements PMT and is absent from most assessments of the contemporary PMT model. We find support for PsyCap's relationship with the mechanisms of PMT and suggest opportunities to develop PsyCap in conjunction with other organizational security efforts. We present our findings, discuss their implications for research and practice, and highlight several opportunities for future research.

1. Introduction

Information systems (IS) protection is a primary focus of many organizations due to their increased reliance on IS for their success (Crossler et al., 2013; Hsu, Shih, Hung, & Lowry, 2015). The need for technical security measures has been well established and documented in the literature (Zafar & Clark, 2009); however, an evolving view holds that effective information security requires a behavioral, as well as a technical, component (AlHogail, 2015; Boss, Galletta, Lowry, Moody, & Polak, 2015; Hsu et al., 2015; Posey, Roberts, Lowry, Bennett, & Courtney, 2013; Stanton, Stam, Mastrangelo, & Jolton, 2006; Vance, Lowry, & Eggett, 2015). Behavioral considerations in IS security have been exacerbated by the need to provide employees with access to organizational IS throughout the organization via enterprise-wide systems from home and on mobile devices (Cisco, 2013; Vance et al., 2015). This complex security environment blunts the effectiveness of a centralized response from organizational information technology (IT) personnel because the devices and users are often far beyond the proximate control of the IT security staff, and some wide-access systems can never be fully locked down without causing organizational inefficiencies (Vance et al., 2015).

Therefore, many researchers in information security now recognize that an organization's information security depends increasingly on the security efforts of organizational insiders who have access to the firm's IS (D'Arcy & Hovav, 2007; Hsu et al., 2015; Vance et al., 2015). These *insiders* are full-time and part-time employees, as well as authorized agents of the firm, with access to the organization's information assets (Moore, Hanley, & Mundie, 2012; Posey et al., 2013). This evolving influence of the insider has led to the emergence of behavioral information security (Crossler et al., 2013), which is the study of "the human actions that influence the availability, confidentiality, and integrity of information systems" (Stanton et al., 2006, p. 263). Unfortunately, identifying the

* Corresponding author.
E-mail addresses: aburns@uttyler.edu (A.J. Burns), cposey@cba.ua.edu (C. Posey), troberts2@uttyler.edu (T.L. Roberts), Paul.Lowry.PhD@gmail.com (P. Benjamin Lowry).

http://dx.doi.org/10.1016/j.chb.2016.11.018
0747-5632/

motivators of these important behaviors has proved to be somewhat elusive, resulting in what the discipline has dubbed a "knowing-doing" gap between insiders' abilities and behaviors (Workman, Bommer, & Straub, 2008).

To address this divide separating insiders' knowledge and abilities from security-related behaviors, we look to insights from the positive psychology movement to augment the field's understanding of insiders' performance of protective behaviors. *Positive psychology* is a branch of psychology that considers the "optimal functioning of people, groups, and institutions" (Gable & Haidt, 2005, p. 104) and seeks to improve what is *right* rather than fix what is *wrong* in the average person (Sheldon & King, 2001). Consequently, we assert that integrating positive psychology with current IS security approaches can improve their explanation of security-related outcomes, particularly those outcomes directly resulting from insiders' behaviors. To demonstrate the role of positive psychology in IS security, we assess the motivational facets from the established motivational framework of protection motivation theory (PMT) (Floyd, Prentice-Dunn, & Rogers, 2000; Rogers & Prentice-Dunn, 1997) that are used extensively in information security (e.g., Boss et al., 2015; Posey, Roberts, & Lowry, 2015a), in relation to a work-related core tenet of positive psychology, psychological capital (PsyCap) (Luthans, Vogelgesang, & Lester, 2006b; Luthans, Youssef, & Avolio, 2007b).

PsyCap is a higher-order construct comprising the work-related, role-breadth tenets of positive psychology: hope, optimism, resilience, and self-efficacy (Luthans, Avey, Avolio, Norman, & Combs, 2006a; Seligman & Csikszentmihalyi, 2000). Role-breadth resources, such as PsyCap, are uniquely positioned for use in contemporary organizational IS security research because they relate to a broader set of tasks rather than an employee's technical job requirements (Parker, 1998). Our integration of PsyCap with PMT is in line with the view of PMT's founders that the consideration of positive outcomes increases the theory's applicability without substantially modifying its core tenets (Maddux & Rogers, 1983). Accordingly, we assert that examining the relationship of PsyCap with the core appeals (i.e., threat and coping appraisals) suggested by PMT (Rogers, 1975; 1983) provides an important updated consideration of the prominent theory's explanation of insiders' performance of protective-based actions, such as protection-motivated behaviors (PMBs). *PMBs* are the volitional behaviors organizational insiders can enact to protect (1) organizationally relevant information within their firms and (2) the computer-based IS that stores, collects, disseminates, and/or manipulates that information in light of information security threats (Posey et al., 2013).

2. Background on Psychological Capital (PsyCap)

As a higher-order construct, PsyCap comprises several distinct, yet related, core tenets of positive psychology: hope, resilience, optimism, and self-efficacy. Positive psychology focuses on optimal functioning or what is known as "flourishing" (Seligman & Csikszentmihalyi, 2000). Positive psychology is an ideal complement to IS security research because its emphasis on the positive functioning of average people (Sheldon & King, 2001) makes it well-calibrated for investigations of information security-enhancing behaviors of ordinary employees. Further, PsyCap introduces an important broad-based, work-related positive psychological resource to the IS security literature, which is still grappling with a knowing-doing gap (Cox, 2012; Workman et al., 2008).

Hope, the first of the four PsyCap subconstructs, is a "positive motivational state that is based on an interactively derived sense of successful (a) agency (goal-directed energy) and (b) pathways (planning to meet goals)" (Snyder, Irving, & Anderson, 1991, p. 287). PsyCap *resilience* "is characterized by positive coping and adaptation in the face of significant risk or adversity" (Luthans, Avolio, Avey, & Norman, 2007a, p. 546). Resilience is also "the positive psychological capacity to rebound, to 'bounce back' from adversity, uncertainty, conflict, failure, or even positive change, progress and increased responsibility" (Luthans, 2002, p. 702). PsyCap *optimism* is the characteristic of individuals who "expect things to go their way, and generally believe that good rather than bad things will happen to them" (Scheier & Carver, 1985, p. 219). Finally, PsyCap *self-efficacy* is a role-breadth characteristic and is defined as an "employee's perceived capability of carrying out a broader and more proactive set of work tasks that extend beyond prescribed technical requirements" (Parker, 1998, p. 835).

Although a relatively new construct, PsyCap has already been well accepted in the field of organizational behavior and other fields (Abbas, Raja, Darr, & Bouckenooghe, 2014; Avey, Luthans, & Jensen, 2009; Peterson, Luthans, Avolio, Walumbwa, & Zhang, 2011; Wang, Liu, Wang, & Wang, 2012). A primary reason for this acceptance is that PsyCap's characteristics are state-like rather than trait-like. Although research often relies on context to infer distinctions between states and traits (Allen & Potkay, 1981), important distinctions exist between them (Fugate, Prussia, & Kinicki, 2012; Zuckerman, 1983). As opposed to *trait-like* individual characteristics, which tend to be relatively stable and pervasive, *state-like* characteristics relate to specific contexts or tasks and may be subject to change over time (Chen, Gully, Whiteman, & Kilcullen, 2000). The key aspect of individual *state-like* characteristics is they can be changed and altered depending on the task, situation, and environment. This distinction is especially beneficial in an information security context because studies show individuals can develop PsyCap (Luthans et al., 2007a; Peterson et al., 2011). The ductile quality of PsyCap and its components distinguishes them from other more stable, trait-like personal characteristics, such as the "Big Five" personality facets (Goldberg, 1990) and the higher-order construct of core self-evaluation (Judge & Bono, 2001; Luthans et al., 2007a). Peterson (2012) summarizes PsyCap's state-like nature succinctly:

> People's locus of control and self-esteem are things a manager probably can't change significantly within a few weeks. Psychological capital is more malleable. We're not born hopeful, resilient, optimistic, efficacious people. We learn these things.

State-like malleability is a crucial aspect of PsyCap because it allows intervention in an individual's course of action. Thus, the mechanisms for developing insiders' PsyCap constitute a key aspect of its applicability for IS security. For example, PsyCap can be developed within the organization through targeted interventions (i.e., developed at the subconstruct level) (Luthans et al., 2006a, 2006b) or as a higher-order factor through broader means (e.g., supportive organizational climate) (Luthans, Norman, Avolio, & Avey, 2008b). Researchers who have conducted targeted intervention research efforts, termed *PsyCap interventions*, have enumerated successful strategies for developing PsyCap in the workplace (Luthans et al., 2007a, 2008b). A thorough treatment of PsyCap "micro-intervention" appears in Luthans et al. (2007a). Table 1 summarizes possible PsyCap interventions.

PsyCap is a higher-order reflective construct, which means that its subconstructs vary together in the same direction (Bagozzi, 2011; Jarvis, MacKenzie, & Podsakoff, 2003). Building PsyCap at the subconstruct level leverages the synergistic relationship among the individual components to develop each subconstruct simultaneously (Luthans et al., 2007b). As the name implies, one can relate PsyCap to a factor of psychological production. Parallel with the