The current reference for this work is as follows:

> *A. J. Burns, Tom L. Roberts, Clay Posey, and Paul Benjamin Lowry (2016). "Examining the influence of organisational insiders' psychological capital on information security threat and coping appraisals," ***Computers in Human Behavior (CHB)*** (accepted 12-Nov-2016)
>
> * = corresponding author

If you have any questions, would like a copy of the final version of the article, or would like copies of other articles we've published, please contact any of us directly, as follows:

- **Dr. A. J. Burns**
  - Email: ajburnsiii@gmail.com
  - Website: http://www.uttyler.edu/directory/cs/burns.php
- **Dr. Clay Posey:**
  - Email: mcposey@yahoo.com
  - Website: http://cba.ua.edu/faculty/profile/370
- **Prof. Tom L. Roberts:**
  - Email: tlroberts17@yahoo.com
  - Website: http://www.uttyler.edu/directory/cs/troberts.php
- **Prof. Paul Benjamin Lowry**
  - Email: Paul.Lowry.PhD@gmail.com
  - Website: https://sites.google.com/site/professorlowrypaulbenjamin/home
  - System to request Paul's articles: https://seanacademic.qualtrics.com/SE/?SID=SV_7WCaP0V7FA0GWWx

Examining the Relationship of Organizational Insiders' Psychological Capital with Information Security Threat and Coping Appraisals

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.

Keywords

Information security, psychological capital (PsyCap), protection motivation theory (PMT), positive psychology, organizational insiders

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 et al., 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 et al., 2015; Hsu et al., 2015; Posey et al., 2013; Stanton et al., 2006; Vance et al., 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 et al., 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 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 et al., 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 et al., 2000; Rogers & Prentice-Dunn, 1997) that are used extensively in information security (e.g., Boss et al., 2015; Posey et al., 2015a), in relation to a work-related core tenet of positive psychology, psychological capital (PsyCap) (Luthans et al., 2006b; Luthans et al., 2007b).

PsyCap is a higher-order construct comprising the work-related, role-breadth tenets of positive psychology: hope, optimism, resilience, and self-efficacy (Luthans et al., 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 et al., 1991, p. 287) . PsyCap *resilience* "is characterized by positive coping and adaptation in the face of significant risk or adversity" (Luthans et al., 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 et al., 2014; Avey et al., 2009; Peterson et al., 2011; Wang et al., 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 et al., 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 et al., 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; Luthans et al., 2006b) or as a higher-order factor through broader means (e.g., supportive organizational climate) (Luthans et al., 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; Luthans et al., 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 et al., 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

Table 1. Micro-developments and PsyCap Interventions[i]

PsyCap Component	Micro-developments	PsyCap Interventions Strategies
Hope	1. Goal setting 2. Participation 3. Contingency planning for alternative pathways to attain goals	1. Encourage employees to define personally valuable work-related goals. 2. Empower goal ownership. 3. Assist in obstacle prediction and develop contingency plans for achievement.
Resilience	1. Asset-focused strategies, such as enhancing employability 2. Risk-focused strategies, such as proactive avoidance of adversity 3. Process-focused strategies to influence the interpretation of adverse events	1. Train employees with transferable skills to enhance perception of work-related assets. 2. Help identify roadblocks and avenues of avoidance. 3. Coach employees to frame setbacks in terms of impact, control, and options to guard against feelings of helplessness and encourage ability to bounce back in the face of adversity.
Optimism	1. Leniency for the past 2. Appreciation for the present 3. Identifying future opportunities	1. Encourage problem-centered coping that acknowledges the sunk-cost of past failures. 2. Characterize the present as an opportunity for success. 3. Counteract pessimism through the development of realistic, yet optimistic, expectations.
Self-Efficacy	1. Mastery experiences 2. Modelling and vicarious learning 3. Social persuasion 4. Physiological and psychological arousal	1. Enable "small successes" by breaking down overarching goals into achievable intermediate tasks. 2. Develop training and mentorship programs that allow employees to observe success and learn from others' failures. 3. Provide positive feedback. 4. Support employees' well-being by minimizing unnecessary workplace stressors.

[i] Adapted from descriptions by Luthans et al. (2006a); Luthans et al. (2008a); Luthans et al. (2007a).

psychological production. Parallel with the traditional factors of economic production, such as land (or natural resources), labor, and capital (Beer, 1980; Huettner & Costanza, 1982), PsyCap meets the criteria of a psychological resource (Avey et al., 2009). A *resource* can be defined as "those entities that are either centrally valued in their own right (e.g., self-esteem, close attachments, health, and inner peace) or act as a means to obtain centrally valued ends (e.g., money, social support, and credit)" (Hobfoll, 2002, p. 307). Therefore, an appropriate theoretical lens through which to view PsyCap is that of resource theory (Hobfoll, 1989, 2002; Luthans et al., 2007b). Hobfoll's (1989) resource theory stipulates that individuals require resources to function and seek to gain available resources and, whenever possible, conserve them. Thus, the conservation of resources theory has two major foci: (1) resource attainment and creation and

(2) resource conservation. In terms of Hobfoll's resource definition, PsyCap is adaptive because it not only embodies a positive psychological state, but it also serves meaningful ends as a psychological construct. For instance, previous research shows that PsyCap provides the requisite psychological capacity or resources for psychological well-being and positive functioning (Culbertson et al., 2010).

Whether one views PsyCap as a psychological resource or simply as a psychological state, it is important to highlight the previously established links between PsyCap and organizational outcomes. For our purposes, it is also imperative to relate the established relationships of PsyCap to IS security and PMT. First, the existing body of PsyCap literature has uncovered a positive relationship between PsyCap and increases in *positive* organizational and personal outcomes, as well as decreases in *negative* organizational and personal outcomes. For example, studies show that PsyCap increases job performance and satisfaction (Luthans et al., 2007a), as well as organizational commitment and citizenship (Avey et al., 2011). These previous findings are important because a positive relationship between satisfaction and organizational citizenship behaviors (i.e., in- and extra-role behaviors that support the organization) exists (Bateman & Organ, 1983; Williams & Anderson, 1991). Conversely, studies show PsyCap reduces unfavorable outcomes, such as absenteeism (Avey et al., 2006), turnover and stress (Avey et al., 2009), and cynicism and deviance (Avey et al., 2011).

Therefore, we expect that as a domain-specific set of in- and extra-role security behaviors, PMBs similarly relate positively with insiders' PsyCap. In light of the established organizational and personal implications of employees' PsyCap, we hypothesize that the incorporation of PsyCap with IS security efforts will result in a symbiotic relationship between positive organizational and security outcomes.

3. Background on Protection Motivation Theory (PMT)

Researchers have employed PMT to assist in understanding individuals' protective intentions and behaviors in varied motivational settings (Floyd et al., 2000; Milne et al., 2000), including IS security research (Anderson & Agarwal, 2010; Herath & Rao, 2009; Johnston & Warkentin, 2010; LaRose et al., 2008; Lee & Larsen, 2009; Pahnila et al., 2007; Woon et al., 2005; Workman et al., 2008). Most previous

PMT efforts in IS security research relied on partial nomologies and implementations of PMT, which oversight has been recently corrected by Boss et al. (2015) and Posey et al. (2015a). Previous IS security studies have used PMT to assess the motivation related to various security-related intentions and behaviors. For example, PMT has been applied to the protection of personal resources from information security threats by motivating behaviors related to the adoption of home wireless security systems (Woon et al., 2005), anti-spyware/anti-malware software on personal computers (Gurung et al., 2009; Lee & Larsen, 2009), and location-based services (Junglas et al., 2008).

Researchers have also effectively tapped PMT to explore employees' intentions to protect organizational resources by adopting virus-protection software at work (Lee & Kozar, 2008), performing basic computer-security operations at work (e.g., updating passwords, securely backing up important files, and updating virus-protection software) (Workman et al., 2008), and complying with organizational information security policies (Herath & Rao, 2009; Siponen et al., 2009; 2010). These studies explaining employees' security-related intentions and behaviors build on previous research explaining PMT's role in understanding organizational issues, such as institutional change (Welbourne & Felton, 1998), employees' reactions to social problems within the organization (Tanner et al., 1989), and the protection of organizations from financial losses (Beck, 1984).

For our research, we examine PMT components as motivating factors for insiders to engage in PMBs. As previously defined, PMBs are a general class of protective roles that can capture both in-role and extra-role behaviors, which are generalizable across positions and industries. As a global measure, PMBs represent all insiders' behaviors that aim to protect the organization, irrespective of the formally specified security needs of individual firms.

In its original conception as an appeal to fear, PMT consisted of three major considerations: "(a) the magnitude of noxiousness of a depicted event; (b) the probability of that event's occurrence; and (c) the efficacy of a protective response" (Rogers, 1975, p. 93). PMT later evolved to include what others describe as efficacy expectations (i.e., Bandura, 1977), or simply the *self-efficacy*, of the motivated individual (Maddux & Rogers, 1983). The original inclusion of self-efficacy framed PMT as a general motivation theory, or theory of attitude change, rather than as a theory relying solely on fear appeals for change (Maddux & Rogers, 1983). Whereas prior to the inclusion of self-efficacy, PMT had a primarily external focus, with the inclusion of self-efficacy, PMT now includes a component that is both positive and internal to the motivated actor.

Consequently, to guide our work, we use the latest adaptations of PMT: a bifurcated approach consisting of a threat appraisal and a coping appraisal. The threat appraisal includes: (1) the perceived probability that a threat will be successful (i.e., *threat vulnerability*); (2) the perceived acuteness of a threat's consequences (i.e., *threat severity*); and (3) the perceived benefits to not enacting a prescribed response to a threat (i.e., *maladaptive rewards*) (Maddux & Rogers, 1983; Rippetoe & Rogers, 1987). Additionally, contemporary PMT studies position fear as a partial mediator between the two threat-focused coping mechanisms (i.e., threat severity and threat vulnerability) and behavioral adaptation (Floyd et al., 2000; Rogers & Prentice-Dunn, 1997). This conceptualization of fear has been employed by IS researchers as well (Boss et al., 2015; Posey et al., 2015a). In the context of fear appeals, we define *fear* as a high-arousal, negative emotion occurring in response to threatening, relevant stimuli (Witte, 1992). Conversely, the coping appraisal includes: (1) the perceived effectiveness of the available response (i.e., *response efficacy*); (2) the perceived ability to enact the prescribed response (i.e., *self-efficacy*); and (3) the perceived costs to the individual, both in terms of expended resources and opportunity cost from enacting a prescribed response (i.e., *response cost*) (Rogers, 1983; Rogers & Prentice-Dunn, 1997).

Despite the role of positive motivation resulting from PMT's inclusion of self-efficacy, even the most up-to-date conceptualizations of the theory fail to include role-breadth resources which are applicable across the gamut of behaviors of a particular domain. This limitation is especially relevant in today's technological organizations, which often call on insiders to enact one of a range of protective behaviors to protect the firm's resources. For example, Posey et al. (2013) established the diverse behavioral set that comprises insiders' potential for protecting organizations from information security threats. Every insider has a portfolio of protective roles and associated behaviors with which they must engage to protect organizational information assets. In the information security context, these roles vary depending on the situation. This set of roles provides a wide range of possibilities; yet, attending to divergent demands requires the insider to employ significant role-breadth resources (Smith & Lewis, 2011). Traditional PMT cannot address this role-breadth nature of emerging security roles, and it is currently unclear how positive resource capabilities, such as those comprising PsyCap, relate to the facets of PMT. Consequently, examining PsyCap's relationship with the facets of PMT serves as an important calibration of PMT to account for a broadened set of roles in PMBs.

Both in terms of PsyCap's potential relationship with PMT and PMT's role in motivating PMBs, the distinction between the coping appraisal and threat appraisal is important. Despite the potential for positive management of the threat that the coping appraisal provides, the prevailing perspective of PMT has been in line with its earliest conceptualization as an approach to motivation through a fear appeal. In fact, security conceptualizations have largely ignored positive coping, such as self-efficacy, and have focused on security motivation purely in terms of fear appeals, while excluding fear itself (e.g., Johnston & Warkentin, 2010). The results of studies incorporating a fear appeal have clearly shown that fear appeals offer explanations of an insider's intention to perform security behaviors (Herath & Rao, 2009; Johnston & Warkentin, 2010); yet, the presence of a fear response has recently been challenged (Warkentin et al., 2016). Meta-analyses of PMT research have shown that across studies of PMT, the coping appraisal has been more effective than the threat appraisal in eliciting the desired response (Floyd et al., 2000; Milne et al., 2000). Furthermore, we expect PsyCap, as a role-breadth construct of positive resource capabilities, to positively relate to the efficacy-based facets of the coping appraisal (i.e., security self-efficacy and response efficacy), while negatively relating to other facets (e.g., reducing threat severity by virtue of its hopeful, optimistic, self-efficacious, and resilient qualities). We will discuss these relationships in more detail through the development of our hypotheses in the next section.

As noted previously, several researchers have applied portions of PMT to this context because of the theory's natural application to IS security (e.g., Herath & Rao, 2009; Johnston & Warkentin, 2010; Lee & Larsen, 2009; Liang & Xue, 2010). Building on these studies, which have made notable contributions to PMT and IS security research stream, we examine a PMT model that includes the role-breadth PsyCap as an antecedent. Based on the preceding discussion of PsyCap and PMT, we conclude that investigating the relationship of PsyCap with the components of PMT represents a unique opportunity to situate a traditional security approach within the emerging context of positive psychology. Figure 1 displays our conceptual model.

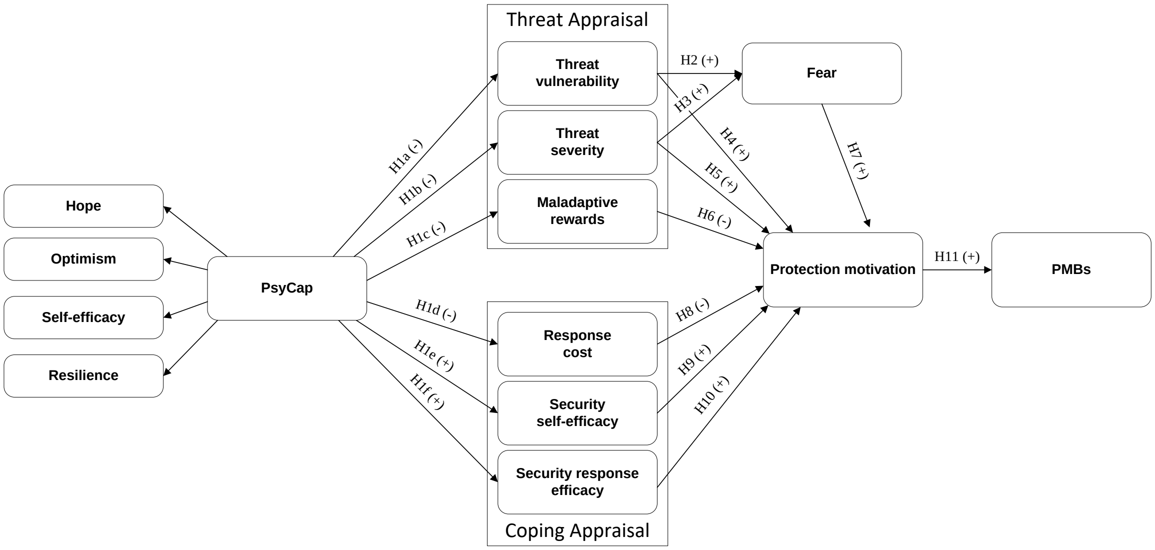


Figure 1. Hypotheses for Research Model

4. PsyCap and PMT Model Hypotheses

As discussed, we expect several distinct mechanisms of PMT to relate to PMB enactment. However, researchers have yet to examine these facets of PMT in the context of role-breadth positive psychological resources such as those in PsyCap. Based on previously established relationships among PsyCap and related constructs, along with its theoretical underpinnings, there are compelling reasons to expect that PsyCap will be related to the mechanisms of PMT. In this section, we first develop hypotheses relating PsyCap to PMT's mechanisms and then offer hypotheses relating PMT to protection motivation and, ultimately, PMBs. We begin by relating PsyCap to the threat appraisal of PMT.

4.1 PsyCap and Threat Appraisal

When insiders are confronted with a threat, they make several assessments regarding its potential ramifications for their organization's information security. Previous research supports PsyCap's potential relationship with the threat appraisal perceptions through the relationship of PsyCap subconstructs with the respective perceptions invoked in the PMT mechanisms. For example, perceptions of threat vulnerability and threat severity relate similarly to the PsyCap subconstructs. First, hope in the security context reflects the perception that the organization can achieve its goals regardless of threats that can affect it. Optimism should also reduce the perception of organizational security vulnerability and severity through the expectation of good rather than bad outcomes. Resilience indicates insiders' abilities to "bounce back" after a negative event and should reduce the perception of the impact of an organizational threat. In other words, resilience characterizes the perception that the organization is able to overcome the threat and, if affected, recover and return to normalcy. Finally, role-breadth self-efficacy details insiders' confidence in their abilities to handle the full breadth of their particular organizational role, including security behaviors and the reaction to negative events and potential organizational threats. Therefore, we hypothesize that PsyCap is negatively related to threat-focused assessments of threat vulnerability and severity.

H1a: Insiders' PsyCap is negatively related to their perceptions of threat vulnerability.

H1b: Insiders' PsyCap is negatively related to their perceptions of threat severity.

Rounding out the threat appraisal process is the perception of maladaptive rewards. As we noted previously, these rewards are perceived benefits an insider may gain from failing to adapt behavior in the intended (i.e., "adaptive" or "protective") manner (Rogers, 1983; Rogers & Prentice-Dunn, 1997). PsyCap has been shown to relate to individual behaviors that are inconsistent with maladaptation. For example, researchers have established relationships between PsyCap and positive organizational behaviors, such as job performance (Luthans et al., 2007a), citizenship behaviors, and low deviance and counterproductive work behaviors (Avey et al., 2011). Given PsyCap's negative relationship with counterproductive work behaviors, such as maladaptation, we hypothesize that PsyCap is also negatively related to maladaptive rewards perceptions, such as illicit or unsanctioned remuneration, for failing to enact PMBs.

> *H1c: Insiders' PsyCap is negatively related to their perceptions of maladaptive rewards.*

4.2 PsyCap and Coping Appraisal

In addition to threat appraisal mechanisms, insiders also engage in a complementary coping appraisal process. Drawing on previously established relationships among PsyCap subconstructs and insiders' perceptions that make up the coping appraisal, we expect PsyCap to relate to the coping appraisal mechanisms. For example, response cost is the insiders' perceived cost (e.g., inconvenience or opportunity cost) of security behavioral adaptations. The established relationships between PsyCap and positive organizational behaviors, such as increased organizational citizenship, imply a reduced perceived response cost in adapting behavior to protect the organization. In other words, an insider with higher PsyCap should calculate fewer response costs than one with low PsyCap. Thus, we hypothesize a negative relationship between PsyCap and security response cost.

> *H1d: Insiders' PsyCap is negatively related to their perceptions of response costs associated with protecting the organization by means of PMBs.*

Further, the two remaining mechanisms of the coping appraisal, self-efficacy and response efficacy, also relate to the subconstructs of PsyCap. As we have noted, in our context, self-efficacy is insiders' confidence in their abilities to take precautions against a security threat, whereas response efficacy is insiders' confidence that precautions they take are effective in protecting their firm's information security. As a role-breadth resource of positive psychological capabilities, PsyCap is likely to have a unique relationship with these efficacy-based components of PMT. For example, through its relationship on positive expectations (Scheier & Carver, 1985), optimism should build confidence in successful behavioral adaptation (i.e., self-efficacy) and behavioral outcomes (i.e., response efficacy). Similarly, resilience builds self- and response efficacy by buffering the demoralizing effect of past loss and/or failure, enabling insiders to bounce back from adversity (Luthans, 2002). Further, as we defined previously, *role-breadth efficacy* is insiders' confidence in performing a broader set of work tasks (often required in the workplace) beyond the technical requirements of their specific job roles (Parker, 1998). Hence, in the context of information security, PsyCap's work-related, role-breadth efficacy should relate positively to the narrower security-related self-efficacy because it pertains to the broad set of security roles insiders assume in fulfilling organizational duties. Finally, hope also includes both agency and pathways for meeting goals (Snyder et al., 1991; Snyder et al., 1996) and should relate directly to perceptions of both self- and response efficacy of protective behaviors.

H1e: Insiders' PsyCap is positively related to their perceptions of security self-efficacy.

H1f: Insiders' PsyCap is positively related to their perceptions of response efficacy.

4.3 PMT Model Hypotheses

The influence of fear appeals on motivation has been widely studied (Witte & Allen, 2000). Although the results have been somewhat equivocal (Peters et al., 2013), the prevailing view is that fear appeals often engage a cognitive processing model (e.g., Leventhal, 1970; Witte, 1992). These process models posit that in response to fear-inducing stimuli, individuals process their reactions largely in one of two ways (or in both ways simultaneously, with the stronger of the two ultimately guiding the response). The two processes are "danger control" and "fear control" (Nabi et al., 2008; Witte, 1994).

The danger control process shares features with the primary cognitive appraisal process described in theories of stress and coping (i.e., Folkman et al., 1986). The primary cognitive appraisal in which individuals engage when confronted with a stressful situation is essentially an appraisal of threat vulnerability, and the motivation to consider the threat further hinges on their perception of existential vulnerability (Folkman et al., 1986). PMT predicts that individuals who focus primarily on controlling danger are more motivated to deal with the cause of the danger, ceteris paribus; that is, a given threat is seen as relevant to a person and generates fear that acts as a motivator, not a de-motivator, because of the complementary positive coping response. Thus, as Figure 1 depicts, the perception of *threat vulnerability* and *threat severity* increases insiders' *protection motivation* and *fear* responses in relation to organizational security threats.

> *H2: Insiders' perceptions of threat vulnerability are positively related to fear.*
>
> *H3: Insiders' perceptions of threat severity are positively related to fear.*
>
> *H4: Insiders' perceptions of threat vulnerability are positively related to their protection motivation.*
>
> *H5: Insiders' perceptions of threat severity are positively related to their protection motivation.*

PMT includes the recognition that not every response to organizational threats is adaptive. This may result from insiders' beliefs that the organization is impervious, the threat is not credible, or the personal benefit of failing to adapt outweighs that of adaptation (termed *maladaptive response*). We model the potential benefit received for failure to enact an adaptive, protective response as *maladaptive rewards* in Figure 1. These rewards may be *intrinsic* or *extrinsic* (Deci, 1972). "Fear control" is an example of a process in which insiders seek a maladaptive reward because they seek the reward of having their fear assuaged without addressing the threat itself. Again, this process involves the classic maladaptive responses researchers have described as avoidance, denial, and reactance (Witte & Allen, 2000), in which negative responses can negatively undermine organizational security compliance and behaviors (Lowry & Moody, 2015; Lowry et al., 2015).

A related form of maladaptive behavior occurs when participants use neutralization techniques (e.g., denial) to rationalize their inappropriate security behaviors (Siponen & Vance, 2010). Maladaptive rewards are internal mechanisms for behavioral justification, but they may also arise externally (i.e., extrinsic rewards). An example of an extrinsic reward is the promise (and/or receipt) of monetary compensation or other enrichment for failing to make an adaptive response. In the context of a security study, one can easily conceive that nefarious actors may be willing to pay an insider for failing to protect the system or even for proactively rendering the system more vulnerable (e.g., sharing login information or selling valuable information).

H6: Insiders' perceptions of maladaptive rewards are negatively related to their protection motivation.

Fear appeals research is predicated on the assumption that a conditioned fear response can elicit a positively adaptive behavior (Boss et al., 2015; Johnston & Warkentin, 2010); therefore, in line with previous research, we also include fear's positive relationship with protection motivation (Floyd et al., 2000; Milne et al., 2000).

H7: Fear generated from insiders' perceptions of organizational security threats is positively related to their protection motivation.

PMT also recognizes the influence of the cost of performing the motivated behavior, including the opportunity cost (Rippetoe & Rogers, 1987). *Response cost* "may include expense, inconvenience, difficulty, and the side effects of the recommended response or of the actions associated with making that response" (Fruin et al., 1992, p. 57). The higher the perceived cost, the less motivated an individual is to perform the desired behavior.

H8: Insiders' perceptions of the response cost associated with protective behaviors is negatively related to their protection motivation.

As we mentioned, PMT's coping appraisal includes individuals' beliefs that they are able to enact a prescribed response (e.g., security self-efficacy). The influence of self-efficacy on security-related motivation stems from Bandura's work and is supported in previous PMT-based studies as well as other motivational theories (Bulgurcu et al., 2010; Herath & Rao, 2009; Johnston & Warkentin, 2010; Milne et al., 2000). Thus, we include security self-efficacy as an antecedent to protection motivation.

H9: Insiders' perceptions of security self-efficacy is positively related to their protection motivation.

Researchers have long considered individuals' perceptions of the efficacy of a desired response to have a motivational influence. Seminal works on efficacy have described the motivational influence of efficacy in terms of a dual model consisting of the efficacy of self and the efficacy of response (Bandura, 1977). Similarly, expectancies have been described as involving both an *action-outcome association* and an *outcome-outcome association* (Vroom, 1964). From this perspective, motivation depends on individuals' beliefs that with effort they can enact a response (action leads to outcome) and, further, that the response they enact ultimately brings about the desired result (efficacy of the response). This latter expectancy has been a fundamental part of PMT since its inception, and we hypothesize individuals' perceptions of response efficacy relates positively to their protection motivation.

> *H10: Insiders' perceptions of response efficacy is positively related to their protection motivation.*

The scope of PMT includes the factors that increase motivation (i.e., protection motivation) and ultimately lead to behavioral elicitation (Rogers & Prentice-Dunn, 1997). However, this does not mean that measuring behaviors along with protection motivation is incongruous with PMT. The role of intentions in PMT parallels their role in other prominent behavioral theories, such as the theories of reasoned action and planned behavior (e.g., Ajzen, 1991; Ajzen & Fishbein, 1972), which assert that intentions often mediate behaviors. Hence, the point of PMT is to increase the motivation and performance of adaptive behaviors. It is a natural application of PMT to test the relationship between intention and behavior, and previous evaluations have assessed both PMT intentions and behaviors in a variety of contexts. Consequently, we expect protection motivation will be positively related to PMBs.

> *H11: Insiders' protection motivation levels are positively related to insiders' engagement in PMBs.*

5. Research Methodology

To test our model empirically, we surveyed organizational insiders through a panel provided by an online market-research firm. Panels are especially appropriate for gathering security data because they offer full anonymity, not simply confidentiality. Given the sensitive nature of responses regarding security outcomes within organizations, anonymity was necessary to encourage candid responses, and panels provided increased anonymity in multiple ways. First, the researchers never know the identity of respondents, and the data provider guarantees and governs the privacy of respondents. Second, respondents' actual and perceived anonymity is enhanced because they receive access to the survey outside their organizations' networks and computers and because the survey is administered and analyzed outside their organizations. Providing anonymous, off-site access to self-report surveys has been established as a leading method to elicit incidences of sensitive behaviors, such as PMBs (Posey et al., 2013), organizational whistle-blowing (Lowry et al., 2013), increasing accountability of organization insiders (Vance et al., 2013), as well as socially undesirable behaviors, such as computer abuse (Lowry et al., 2015; Lowry et al., 2014) and organizational deviance (Bennett & Robinson, 2000, 2003). Methodologists also recommend these conditions to eliminate potential common-method biases (Podsakoff et al., 2003).

Because this study examines the security-related behaviors of insiders, we requested responses from a panel of employed insiders working in both the public and private sectors in the U.S. Using online panels also increases certainty that the sampled population represents the targeted population, and explicitly targeting insiders makes the findings more likely to be generalizable to the entire population of insiders. Initially, we received responses from 522 organizational insiders. After excluding incomplete responses and screening for non-conscientious responding (e.g., straight-ticket responding), our final sample was 377 respondents. This figure equates to a usable-to-collected response rate of 72.2%, which meets or exceeds the rate of other similar research (D'Arcy et al., 2014). As recommended, none of the respondents in our retained sample had missing values for greater than 5% of all items, and we employed mean replacement for all missing values (Hair et al., 2014). Further, our sample size surpassed the minimum threshold for detecting weak effects (i.e., $R^2 = 0.10$; $\alpha = 0.01$; power = 0.80) (Cohen, 1992). In our final sample, the respondents had a mean age of 46 years (SD = 14.51) and a mean organizational tenure of 11 years (SD = 9.56), 51% were female, and 58% had at least an undergraduate degree. Additionally, 12.2% worked in the IS department of their organization, and 38% reported working in some level of management.

5.1 Study Measures

In this section, we briefly describe the study's measures; we present the full measures in Appendix A. We begin with a discussion of our measures for the PsyCap higher-order construct. We then consider the threat and coping appraisals separately. Finally, we conclude this section with a discussion of our outcome variables: protection motivation and PMBs.

5.2 PsyCap Construct

We measured *PsyCap* by using items from the previously published PsyCap Questionnaire (Luthans et al., 2007b). The original PsyCap Questionnaire comprises 24 items (six for each of the four characteristics). For this study, we retained at least four items for every underlying characteristic of PsyCap. The items in the PsyCap Questionnaire were adapted by Luthans and colleagues from previous literature to reflect state-like, work-related positive resource capabilities (Luthans et al., 2007a; Luthans et al., 2007b). Specifically, Luthans et al. (2007b) developed the items measuring hope from the State Hope scale (Snyder et al., 1996); the items measuring role-breadth self-efficacy from Parker (1998); the items measuring optimism from Scheier and Carver (1985); and the items measuring resilience from Wagnild and Young (1993). Similar to previous findings using the PsyCap Questionnaire (Avey et al., 2010), we found the subconstructs exhibited sound reliabilities (self-efficacy composite reliability [CR] = 0.90; optimism CR = 0.84; hope CR = 0.88, and resilience CR= 0.80). An example of an item from the PsyCap Questionnaire measuring resilience is “I usually take stressful things at work in stride.”

5.3 Threat Appraisal Constructs

We measured both o*rganizational threat vulnerability* and *threat severity* with items from prior PMT and fear appeals research (Witte et al., 1996; Workman et al., 2008). Similar to findings in recent PMT research using these measures (Posey et al., 2015a), we found strong evidence of validity and reliability of these measures (threat vulnerability CR = 0.91; threat severity CR = 0.92). An item measuring threat vulnerability is “My organization’s information and information systems are vulnerable to security threats.” An example of an item measuring threat severity is “Threats to the security of my organization’s information and information systems are severe.”

We measured *maladaptive rewards* with six items developed and validated in Posey et al. (2010); and Posey et al. (2015a). These items reflect intrinsic and extrinsic benefits an insider may gain from failing to enact PMBs. An example of an item for the extrinsic benefit of maladaptive behavior is "It is likely that I would receive personal rewards for purposefully not protecting my organization's information and information systems from security threats." An example of an item for the intrinsic benefit of maladaptive behavior is "I would feel a sense of internal satisfaction for allowing information security threats to harm my organization." As in prior research (Posey et al., 2010), our maladaptive rewards construct exhibited strong validity and reliability (CR = 0.92).

We measured *fear* by using four items from Block and Keller (1995). This construct has been used in other PMT studies and has exhibited strong reliability (Posey et al., 2015a). To capture insiders' levels of fear of information security threats, we asked them "When thinking about the security threats to your organization's information and information systems, to what extent do you feel…?" An example of an item from the fear scale is "frightened." Similar to the previous PMT study employing fear (Posey et al., 2015a), our measure exhibited strong validity and reliability (CR = 0.95).

5.4 Coping Appraisal Constructs

We measured the coping appraisal constructs, *response efficacy*, *security self-efficacy*, and *response cost*, all with items adapted from previous PMT research (Workman et al., 2008). Each of these measures has exhibited strong reliability in previous PMT studies (Posey et al., 2015a). An example of an item measuring security response efficacy is "Employee efforts to keep my organization's information and information systems safe from information security threats are effective." An example of an item measuring security self-efficacy is "For me, taking information security precautions to protect my organization's information and information systems is easy." An example item measuring response cost is "The inconvenience of implementing recommended security measures to protect my organization's information and information systems exceeds the potential benefits." In our study, as in previous research (Posey et al., 2015a; Workman et al., 2008), we found strong reliabilities for the coping appraisal constructs (security response efficacy CR = 0.87; security self-efficacy CR = 0.83; response cost CR= 0.89).

5.5 Protection Motivation and PMB Constructs

We measured *protection motivation* as an intention to perform protective behaviors (i.e., PMBs), and the scale was developed in accordance with the views of previous behaviorists (e.g., Ajzen & Fishbein, 1972). We drew the three items selected to assess insiders' protection motivations from Posey et al. (2010); and Posey et al. (2015a). An example of an item measuring protection motivation is "I intend to protect my organization from its information security threats." Similar to previous PMT research employing this scale to capture insiders' protection motivations (Posey et al., 2015a), in our study, protection motivation exhibited strong validity and reliability (CR = 0.78).

Finally, we measured *PMBs* with a five-item scale on the basis of the taxonomy of PMBs (Posey et al., 2015b; Posey et al., 2013). This instrument captures insiders' protective security actions across myriad occupations, organizations, and industries; thus, it reflects PMB activity at the overall level. More specifically, in a recent research effort (Posey et al., 2015b), this five-item measure captured more than 70% of the conceptual domain created by 45 unique protective behaviors in nine unique clusters (e.g., account protection, policy-driven awareness and action, protection against unauthorized exposure, and identification and reporting of security matters). An example of an item measuring PMBs is "I actively attempted to protect my organization's information and computerized information systems." Again, as in previous research on insiders' performance of PMBs (Posey et al., 2015a), our PMB construct exhibited strong validity and reliability in our study (CR = 0.96).

6. Analyses and Results

As methodologists recommend, we analyzed the research model in a two-step procedure (Gerbing & Anderson, 1988), and our analysis used the covariance-based structural equation modelling (CB-SEM) platform, Mplus (Muthén & Muthén, 1998-2010). In the first step, we assessed the validity of the measures in the structural model. Upon confirmation of the validity of the research model, we also assessed the hypothesized research model by CB-SEM. As recommended by methodologists (Gefen et al., 2011), before proceeding to our analyses, we first assessed key assumptions about the data by reviewing skewness and kurtosis to assess normality and variance inflation factors (VIFs) to assess collinearity among constructs. We found that in every instance, the VIF was below the most conservative thresholds (Petter et al., 2007), and we found none of the individual kurtosis and skewness values exhibited even moderate levels of non-normality (West et al., 1995). In fact, only one kurtosis value was above an absolute value of 1, with none above 1.4 and only two skewness values were above an absolute value of 1, with none above 1.4. To ensure our SEM model results were conservative, as in prior PMT research (Posey et al., 2015a), we ran our CFA and SEM analyses with a variant of the Maximum Likelihood (ML) estimator in Mplus that produces robust standard errors (MLR) for the ML parameter estimates (Muthén & Muthén, 1998-2010).

6.1 Confirmatory Factor Analysis (CFA)

The validity and reliability of the employed measures are critical to the execution of any study (Gefen et al., 2011; Straub, 1989). Although all scales in this study had been previously used as recommended, per Straub et al. (2004), we assessed instrument validity. For all the measures in the structural model, we considered the standardized factor loadings from a CFA analysis along with the composite reliabilities. Also, we assessed the convergent and discriminant validity of the measures in the structural model with average variance extracted (AVE) and a comparison of squared correlations with AVE, as methodologists recommend (Hair et al., 2006).

We followed the prior literature in conceptualizing PsyCap as a higher-order construct (Luthans et al., 2007a). Specification is a theoretical decision based on the relationship among subconstructs. Luthans et al. (2007a) explain that "multidimensional constructs may have components relating to a core underlying factor whereby the shared variance or commonality between each facet comprises the higher-order factor" (p. 549). A higher-order reflective specification is appropriate where there is a "general or more global factor that explains all the correlations between the first order factors" (Hair et al., 2014, p. 231).

Higher-order constructs have unique requirements compared to first-order measures. To assess the validity of PsyCap as a higher-order construct, we followed the instructions provided by Muthén and Muthén (1998-2010). First, we assessed the lower-order factor validity for each subconstruct separately, then we assessed the subconstruct correlations. For the lower-order subconstructs, the usual metrics for lower-order convergence should be met with AVEs around 0.50 and construct reliabilities around 0.70. However, in contrast to first-order constructs, subconstructs of a higher-order reflective construct do not need to show discriminate validity. Additionally, the number of indicators should be similar across the subconstructs of a higher-order factor (Hair et al., 2014). Our subconstructs exhibited adequate convergence with a range of composite reliabilities of 0.79-0.90 and AVEs ranging between 0.494-0.655. As expected for the subconstructs of a higher-order factor, the PsyCap components were highly correlated with an average correlation of 0.86 and a range of 0.80-0.93, and thus, as suggested by methodologists for higher-order factors (Hair et al., 2014), the lower-order components failed to discriminate.

Next, we continued with our CFA by assessing the validity of the remaining constructs, testing for convergent and discriminant validity as prior research recommends (e.g., Hair et al., 2006). We again considered composite reliabilities to assess the internal consistency of the measures. The range of reliabilities (i.e., 0.78–0.96) met the recommendations of prior research (Nunnally, 1978). We assessed convergent validity by calculating the AVE of each construct, whereas we assessed discriminant validity by comparing the squared correlations with AVE as prior research recommends (Hair et al., 2006). The AVEs were above the recommended value of 0.50 (Hair et al., 2006), ranging from 0.542 to 0.861. All but one pair of constructs met the Fornell-Larcker criterion with a greater AVE than all squared correlations (Hair et al., 2006).

Interestingly, the two highest correlated pairs of constructs in our model were security self-efficacy with security response efficacy (r=0.95) and threat severity with threat vulnerability (r=0.79). These high correlations match those of previous PMT research (i.e., Posey et al., 2015a). Therefore, as recommended by previous researchers who found high correlations among these constructs (Posey et al., 2015a), we opted to drop security self-efficacy and threat vulnerability from our model and proceeded with security response efficacy and threat severity. Our decision to retain security response efficacy and threat severity is further supported by a previous meta-analysis of PMT research, which found these two are more important than their highly correlated counterparts (Rippetoe & Rogers, 1987). For concision, we include the statistics for both our original and refined (i.e., excluding security self-efficacy and threat vulnerability) measurement models at the conclusion of the article in Tables 5 and 6. Our refined CFA model exhibits adequate fit with χ^2 = 1680.968 df =1095; scaling correction factor for MLR = 1.1231; CFI=0.947; TLI =0.944; RMSEA=0.038; SRMR=0.048 (Hu & Bentler, 1999).

6.2 Structural Model

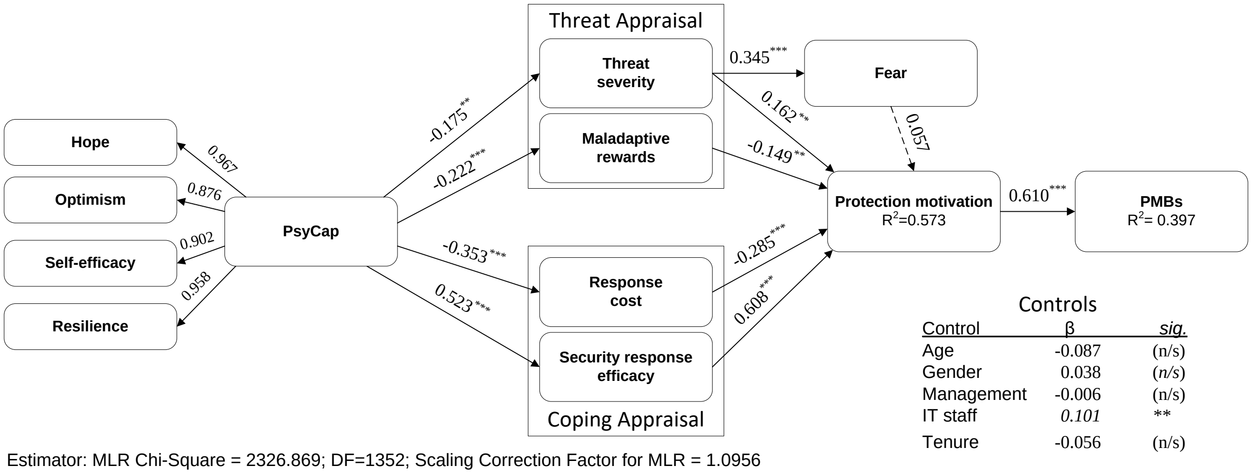
Finally, we assessed the hypothesized relationships. The structural model results are summarized in Table 2, and we present a detailed exhibit of our empirical model (both structural and measurement components) in Figure 3 at the conclusion of the article. As shown in Table 2, the structural model exhibits adequate fit with χ^2 = 1926.706; df = 1112; scaling correction factor for MLR = 1.1256. The CFI and TLI values of 0.927 and 0.923, respectively are both above the recommended level (Gefen et al., 2011). Additionally, the RMSEA value of 0.044 meets the conservative cutoff value for “good” fit (Gefen et al., 2011). We would note that the SRMR value of 0.098 is borderline with regard to the Hu and Bentler (1999) recommendation of “close to 0.08” (p. 1). However, as noted by Gefen et al. (2011), not all fit indices should be expected to be within threshold rules of thumb when multiple indices are reported. Of the 11 hypotheses tested, 10 were supported (i.e., they were significant and in the predicted direction). We report standardized coefficients to aid in the interpretation of our results, which is especially helpful for models with higher-order factors (Bagozzi & Yi, 2012).

Table 2. Structural Model Results

Predicted and Tested Relationship	β Coefficient	t-value (sig.)
H1a. PsyCap → Threat vulnerability	Not examined	
H1b. PsyCap → Threat severity	-0.175	2.802**
H1c. PsyCap → Maladaptive rewards	-0.222	3.854***
H1d. PsyCap → Response cost	-0.353	6.159***
H1e. PsyCap → Security self-efficacy	Not examined	
H1f. PsyCap → Response efficacy	0.523	10.351***
H2. Threat vulnerability → Fear	Not examined	
H3. Threat severity → Fear	0.345	6.671***
H4. Threat vulnerability → Protection motivation	Not examined	
H5. Threat severity → Protection motivation	0.167	3.155**
H6. Maladaptive rewards → Protection motivation	-0.148	2.642**
H7. Fear → Protection motivation	0.053	0.853
H8. Response cost → Protection motivation	-0.283	3.587***
H9. Security self-efficacy → Protection motivation	Not examined	
H10. Response efficacy → Protection motivation	0.609	9.215***
H11. Protection motivation → PMBs	0.595	11.110***

Estimator: MLR Chi-Square = 1926.706 DF=1112; Scaling Correction Factor for MLR = 1.1256
CFI=0.927; TLI=0.923; RMSEA=0.044; SRMR=0.098
*** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$; Protection motivation: $R^2 = 0.571$; PMBs: $R^2 = 0.354$

To establish the robustness of the model, we re-ran our structural model controlling for *age, years of organizational tenure, gender, and whether the respondent had a managerial role and/or was an IT staff member of the organization*. Being an IT staff member was positively related to protection motivation (p = 0.01), whereas all other controls were insignificant. Figure 2 depicts our final structural model results including controls.



Controls

Control	β	*sig.*
Age	-0.087	(n/s)
Gender	0.038	(*n/s*)
Management	-0.006	(n/s)
IT staff	*0.101*	**
Tenure	-0.056	(n/s)

Estimator: MLR Chi-Square = 2326.869; DF=1352; Scaling Correction Factor for MLR = 1.0956
CFI=0.917; TLI=0.913; RMSEA=0.044; SRMR= 0.099
*** p < 0.001, ** p < 0.01, * p < 0.05;

Figure 2. Structural Results Including Controls

6.3 Post-Hoc Analyses

Next, we conducted three post-hoc analyses. First, we conducted formal tests to assess the indirect relationship of PsyCap with protection motivation and PMBs through the PMT mechanisms. Second, we performed a formal test to detect any common method bias (CMV). Third, we assessed the level of protection motivation and PMBs for insiders with relatively high and low PsyCap.

Indirect relationships among variables can be assessed by producing confidence intervals through a resampling, or bootstrap, procedure (MacKinnon et al., 2004). To formally assess the indirect relationships among PsyCap, protection motivation, and PMBs, we constructed bias-controlled 95% confidence intervals using Mplus' *model indirect* procedure (Muthén & Muthén, 1998-2010). Because we found no significant deviations from normality in our data and the direction of our model parameters and significance statistics were the same for both the ML and MLR estimators, we were able to perform indirect analyses using the ML estimator—a requirement in Mplus. As exhibited by (Vance et al., 2015), we ran a bootstrap procedure producing 5,000 resamples to construct bias-controlled confidence intervals. We found significant direct effects for all indirect relationships except the relationships of PsyCap with protection motivation and PMBs via threat severity and fear. Table 3 exhibits the indirect effects.

Table 3. Indirect effects of PsyCap

Bootstrapped CI tests for indirect effects				
	Indirect Effect			
Relationship	2.5%[t] Lower-bound	Estimate	97.5%[t] Upper-bound	Indirect Effect?
PsyCap's relationship with protection motivation (PM)				
PM on *PsyCap* via *threat severity*	-0.055	-0.029	-0.003	Yes
PM on PsyCap via *maladaptive rewards*	0.001	0.033	0.065	Yes
PM on *PsyCap* via *threat severity* and *fear*	-0.012	-0.003	0.005	No
PM on *PsyCap* via *response cost*	0.030	0.100	0.169	Yes
PM on PsyCap via *security response efficacy*	0.214	0.319	0.423	Yes
PsyCap's relationship with PMBs				
PMBs on *PsyCap* via *threat severity* and *PM*	-0.033	-0.017	-0.002	Yes
PMBs on *PsyCap* via *maladaptive rewards* and *PM*	0.001	0.019	0.038	Yes
PMBs on *PsyCap* via *threat severity, fear, and PM*	-0.007	-0.002	0.003	No
PMBs on *PsyCap* via *response cost* and *PM*	0.018	0.059	0.100	Yes
PMBs on *PsyCap* via *security response efficacy* and *PM*	0.114	0.189	0.265	Yes

Estimator: ML Chi-Square = 2168.658 DF=1112; CFI=0.925; TLI=0.921; RMSEA=0.050; SRMR=0.098; resamples=5,000; [t]bias-controlled confidence intervals

As a post-hoc assessment of potential sample bias due to common-method variance (CMV), we followed the procedures for the CFA marker-variable technique previous research recommends (Richardson et al., 2009). CB-SEM is particularly well suited for our chosen CMV analyses, because, unlike other techniques (e.g., unmeasured latent method construct [ULMC] technique), the CFA marker-variable technique specifies the comparison of free and constrained models in a way that allows for appropriate model identification (Liang et al., 2007; Williams et al., 2010). Also, despite being the most frequently used technique, the ULMC has been found to have serious shortcomings in both detecting and correcting CMV (Chin et al., 2012). Conversely, the CFA marker-variable technique, has been found to detect CMV accurately and consistently (Richardson et al., 2009).

With the goal of assessing CMV, we included a marker variable in our survey (i.e., a construct with no theoretical basis for correlation with our substantive constructs). The CFA marker-variable technique uses multiple CFA analyses to test for (1) CMV, (2) unequal (congeneric) method variance, and (3) bias due to CMV. The results of our CFA marker-variable tests indicated no biases in our sample from CMV (see Appendix B).

We also conducted a post-hoc exploration of PsyCap and PMT in which we ran t-tests to examine the level of protection motivation and PMBs for insiders with relatively high and low PsyCap. We found significantly higher levels of protection motivation and PMBs for those with higher PsyCap. We include the results of this post-hoc analysis in Appendix C.

7. Discussion

The burgeoning field of positive psychology has introduced a relatively new paradigm for understanding work-related functioning and motivation. Building on this important foundation, a goal of our study was to assess the relationship of insiders' PsyCap with the traditional information security theory of PMT. Because PMT was originally developed as an appeal to individuals' fears, the relationship between PsyCap and the mechanisms PMT employs were unknown. Drawing on previous studies, we developed hypotheses for PsyCap's varying relationship with the unique PMT facets, including the oftexcluded components of maladaptive rewards and response costs. Interestingly, we found that PsyCap significantly explains variance in each dimension of PMT. In fact, PsyCap works in the same direction as PMT on three of four tested motivational appeals; it relates positively with the positive coping mechanism of security response efficacy and negatively with the negative motivational mechanisms of maladaptive rewards and response cost.

Furthermore, through our post-hoc test for indirect effects, we found support for the relationship of PsyCap with protection motivation and PMBs through PMT's mechanisms. The strongest indirect relationship in our analyses was between PsyCap and protection motivation via security response efficacy. This is an important finding because (1) PyCap has the strongest relationship (in terms of beta coefficient) with security response efficacy of any of the PMT mechanisms, and (2) security response efficacy has the strongest relationship with protection motivation (in terms of beta coefficient) of any PMT mechanism tested in our model. Thus, our findings indicate that PsyCap is most strongly related with the PMT mechanism that has the strongest relationship with protection motivation.

As we hypothesized, however, some of the relationships between PsyCap and PMT do not support the theoretical motivational appeal of PMT. For example, we found that insiders' PsyCap is negatively related to perceptions of threat severity, which were originally conceived in PMT as mechanisms that increase motivation through fear. Despite this potential conflict of motivational view between positive psychology and PMT, as shown in Figure 2, PsyCap does not remove the perception of threat severity's relationship with protection motivation and PMBs (i.e., threat severity retained significance in the model). This is an important point and may actually increase the efficacy of PMT as a whole because overwhelming perceptions of threat severity may lead to a level of fear that is counterproductive to positive motivation and results in insiders' engagement in an avoidance response. Specifically, if fear is too strong (e.g., overwhelms one's efficacy), it can act to narrow the repertoire of behavioral responses cognitively available to the actor (Fredrickson, 2001) and trigger a state of readiness for withdrawal behavior such as "flight" (Bagozzi et al., 1999). For example, helpless feelings stemming from perceptions of insurmountable severity have the potential to elicit maladaptive responses, such as avoidance and/or withdrawal behaviors (Carver & Scheier, 1982; Diener & Dweck, 1980). That is, some threat-related perceptions may lead to adaptive coping and elicit PMBs, whereas others may lead to helpless feelings and maladaptive coping, such as the withdrawal from security roles (Burns et al., 2015).

In our study, we found that threat severity relates positively to fear experienced due to perceptions of organizational information security threats; however, fear does not translate into positive motivation to protect the firm. In other words, we did not find a significant link between fear and protection motivation. While this was not our hypothesized result, it is supported by the results of previous research that challenge the presence of a fear response in relation to the PMT mechanisms (Warkentin et al., 2016). We believe this finding is attributable to the nature of fear in our context. As an emotional response, fear arises from an appraisal of threatening stimuli and engenders a cognitive and physiological reaction (Bagozzi et al., 1999). Further, emotions are transient states (Fredrickson, 2001). Therefore, we assert that the relationship between fear and behavior is more readily observed in the presence of direct fear manipulation at the time of the action than in the “pre-kinetic” level of behavioral intention (Willison & Warkentin, 2013). This was shown by Boss et al. (2015) who used direct fear-appeal manipulations. Our research does not employ direct fear-appeal manipulations, which can be further considered in future PsyCap research.

Importantly, threat vulnerability and threat severity were too highly correlated to both be included in our model. This finding perhaps points to the reality that, in our study, respondents perceived that the more vulnerable the organization is to threats, the more significant are the threats. Finally, through post-hoc analyses, we found that insiders with higher PsyCap report higher levels of protection motivation and PMBs. This finding—in light of the negative relationship between PsyCap and the threat-focused appeals of threat vulnerability and threat severity—points to the strong relationship between the coping appraisal mechanisms in PMT and proactive security-related behaviors (i.e., protection motivation and PMBs). In our study, as in previous studies, we found that the coping appraisal is much more influential in the development of protection motivation levels than is the threat appraisal (i.e., in terms of the magnitude of beta coefficients).

7.1 Implications and Contributions

Our research has important implications for both academicians and practitioners who are interested in eliciting positive security behaviors among organizational insiders. In the context of IS security, PsyCap is simply insiders' psychological resources available to support optimal functioning. As a psychological resource, PsyCap has been shown to be important for organizational and personal outcomes. By considering PsyCap's relationship with the mechanisms of PMT, we calibrate the theory with the evolving perspective that information security is an optimal organizational outcome that insiders across the organization must consider. The positive psychological resources PsyCap embodies are especially important for insider-focused security given current workplace environments, which require insiders to adapt and select (i.e., to differentiate their behavior) from a wide array of activities within a behavioral repertoire of security-focused options (e.g., Posey et al., 2013).

Furthermore, our results indicate that PsyCap enhances the efficacious coping appraisal mechanisms within PMT by increasing security response-efficacy and reducing perceptions of security response costs. PsyCap also acts to decrease perceptions of potential maladaptive rewards for not performing the positive security-oriented activities—an important consideration should insiders actively contemplate personal rewards for not engaging in adaptive responses against organizational security threats.

The introduction of PsyCap into IS security is itself an important contribution because PsyCap contains the state-like elements of positive psychology. Research has shown that individuals can develop these elements and that these elements link to a number of important positive organizational outcomes. PsyCap components offer a unique opportunity to ascertain the synergistic relationship among insiders' characteristics and organizational security, along with other important organizational outcomes, such as job performance and satisfaction (Luthans et al., 2007a), low absenteeism (Avey et al., 2006), and low turnover and stress (Avey et al., 2009). As we discussed previously, each of these outcomes represents security issues within organizations.

Table 4. Improving Organizational Security Efforts with PsyCap Interventions

PsyCap Component	Micro-developments in a Security Context	PCI Strategies
Hope (goal setting)	1. Security goal setting 2. Security participation 3. Security contingency planning	1. Develop specific, reasonable, achievable employee-level goals related to information security (e.g., enactment of PMBs). 2. Include employees in the security goal development process. 3. Tailor SETA efforts to include contingency plans for if/when a security threat arises.
Resilience (positive coping strategies)	1. Security asset-focused strategies 2. Security risk-focused strategies, such as proactive avoidance of adversity 3. Security process-focused strategies	1. Reinforce the transferable value of security-enhancing behaviors in career development. 2. Educate employees on the potential personal work-related benefits (e.g., fewer interruptions, enhanced firm reputation) from enacting PMBs to help the firm avoid information security threats. 3. Encourage employees to incorporate PMBs into their behavioral repertoire step-by-step to increase perceived controllability and effort during adversity.
Optimism (past, present, future)	1. Leniency for the past security failures 2. Appreciation for the present security threats 3. Identifying future opportunities to enhance security	1. Use past security shortcomings as "teachable moments" to encourage future PMBs. 2. Train employees to see current security threats as an opportunity to protect the firm as opposed to an opportunity for failure. 3. Counteract pessimism regarding information security through the development of realistic, yet optimistic, expectations.
Self-efficacy (mastery, persuasion, and arousal)	1. Security mastery experiences 2. Modelling and vicarious learning 3. Security social persuasion 4. Security physiological and psychological arousal	1. Develop SETA efforts that enable "small successes" by breaking down security goals into achievable tasks. 2. Incorporate mentorship activities into SETA programs that allow employees to observe success and learn from others' failures. 3. Provide positive feedback to employees enacting PMBs. 4. Reduce security-related stress by equipping employees with effective response mechanisms and clear policies.

Finally, and perhaps most importantly, as a construct comprising state-like subconstructs, PsyCap provides managers with a model for the design of vetting procedures and subsequent insider training. They can develop insiders' PsyCap at either the subconstruct level or the macro level. Peterson et al. (2011) assert that "employees' level of psychological capital is also subject to change (increase or decrease) depending on the work context such as the amount of social support they receive, leadership, and/or organizational climate" (p. 432). The construct-level development of PsyCap opens the door for research into the antecedents of PsyCap. This opportunity is especially important in light of the present study, which found that PsyCap is related to each component of PMT's threat and coping appraisal mechanisms included in our study. Thus, our broadened PMT approach provides a theoretically sound context in which to establish the relationship between PsyCap and motivational appeals for employees to perform positive security behaviors (i.e., PMBs). To augment these practical implications, we contextualize the PsyCap development strategies in an information security context and offer opportunities for improving organizational security programs with the inclusion of PsyCap interventions in Table 4. These prescriptions should aid organizational managers in the formation, delivery, and maintenance of internal security-related efforts to further enhance the organization's security posture.

Given insiders' unprecedented access to the IS of organizations and organizations' increased foci on the positive psychological aspects of their employees, the investigation of PsyCap's relationship with PMT provides an important contribution to IS security research. The results of this study support the symbiotic relationship between positive psychological factors and organizational security outcomes. Consequently, investments in employees' PsyCap, whether generally (as Table 1 describes) or within a security context (as Table 4 describes), can be thought of as investments in information security.

7.2 Limitations and Future Research

This study offers initial insights into the relationship of PsyCap with a traditional theory in IS security research, PMT. As such, it is not without limitations. Our study focused on the relationship between PsyCap and the traditional PMT model rather than testing additional hypotheses introduced to the base PMT model. Therefore, the PMT model we presented does not include some of the constructs that have been considered alongside PMT, such as social influence (Lee & Larsen, 2009) and descriptive norms (Anderson & Agarwal, 2010), although these are not core PMT constructs. Future research should explore the relationship of PsyCap with extended versions of PMT and other established motivational theories.

PsyCap's state-like characteristics make it uniquely qualified for use in IS security, and it has already been shown to serve as an important mediator (Luthans et al., 2008b) and moderator (Chadwick & Raver, 2013; Cheung et al., 2011) in important individual-organization relationships. Therefore, future IS research considering PsyCap should study not only its relationship with security or other variables of interest, but also the mediating and/or moderating relationship of PsyCap with important IS relationships. PsyCap is also amenable to experimentation, and researchers can study the manipulation of PsyCap, either through micro intervention or by the manipulation of organizational climate perceptions, and measure the resulting influence on IS-related outcomes. Given the malleability of PsyCap and its established relationship with the mechanisms of PMT, research into the antecedents of PsyCap will also offer insights into IS security. Finally, given the relationship of role-breadth, work-related PsyCap with the PMT mechanisms, future research could develop a more targeted measure of PsyCap that captures hope, optimism, efficacy, and resilience as it relates specifically to information security (i.e., a measure of insiders' *security PsyCap*).

As a final possible limitation, the use of panels is not readily amenable to researchers' assessments of intentions and actual behaviors at separate time periods with the same set of participants. Further, the nature of a cross-sectional design makes it much more difficult for researchers to determine when respondents actually formed perceptions and intentions and performed behaviors of interest when compared with highly controlled experimental approaches where researchers can assess the formation of intentions regarding novel phenomena. Therefore, similar to previous research efforts (Liang & Xue, 2010; Pahnila et al., 2007), we chose to assess protection motivation levels (i.e., intentions) and PMBs (i.e., behaviors) in contemporary fashion. This approach assists in dealing with the variation that occurs when intentions change from two measurement time points (i.e., temporal instability of intentions) (Conner & Godin, 2007) and the likelihood that the relationship between intentions and behavior diminishes as time elapses (Ajzen & Fishbein, 1980; Davis, 1989). Additionally, previous research has provided evidence that the association assessed by the contemporary measurement of intentions and behaviors can be higher than the correlation between intentions and behaviors assessed at different time periods (Davis, 1989).

8. Conclusion

Our work extends the IS security literature that examines how to influence employees to engage in protective security actions that improve organizational security. We related this view of insiders to that of the positive psychology movement, which focuses on the optimal functioning of the average person. Drawing on this possibility, we proposed a research model and empirically examined the relationship of insiders' PsyCap with PMT's core mechanisms.

By including PsyCap in concert with PMT, we contextualized a well-established theory in IS security within the emerging perspective of positive psychology—all while retaining its original nomological domain. Assessing the relationship between PsyCap and PMT also reflects advances in the study of human functioning and motivation, providing important motivational antecedents that complement the original PMT model. Additionally, by including PsyCap's role-breadth considerations, we better calibrated PMT to predict role-breadth behaviors (such as PMBs) in insiders' behavioral repertoires. Having established the relationship of PsyCap with insiders' motivations to protect their organizations, our study highlights opportunities for future research into PsyCap and other similar psychological constructs in IS security. Practitioners can draw on these examples to leverage the organizational benefits of positive psychology within the information security function of the organization, and academicians can incorporate these strategies into future research on organizational security programs.

References

Abbas, M., Raja, U., Darr, W., and Bouckenooghe, D. (2014). Combined effects of perceived politics and psychological capital on job satisfaction, turnover intentions, and performance. *Journal of Management*, *40*(7), 1813-1830.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179-211.

Ajzen, I. and Fishbein, M. (1972). Attitudes and normative beliefs as factors influencing behavioral intentions. *Journal of Personality and Social Psychology*, *21*(1), 1-9.

Ajzen, I. and Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behavior*. Englewood-Cliffs, NJ: Prentice Hall.

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*, 567-575.

Allen, B. P. and Potkay, C. R. (1981). On the arbitrary distinction between states and traits. *Journal of Personality and Social Psychology, 41*(5), 916-928.

Anderson, C. L. and Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613-643.

Avey, J. B., Luthans, F., and Jensen, S. M. (2009). Psychological capital: A positive resource for combating employee stress and turnover. *Human Resource Management*, *48*(5), 677-693.

Avey, J. B., Luthans, F., Smith, R. M., and Palmer, N. F. (2010). Impact of positive psychological capital on employee well-being over time. *Journal of occupational health psychology*, *15*(1), 17-28.

Avey, J. B., Patera, J. L., and West, B. J. (2006). The implications of positive psychological capital on employee absenteeism. *Journal of Leadership & Organizational Studies, 13*(2), 42-60.

Avey, J. B., Reichard, R. J., Luthans, F., and Mhatre, K. H. (2011). Meta-analysis of the impact of positive psychological capital on employee attitudes, behaviors, and performance. *Human Resource Development Quarterly, 22*(2), 127-152.

Bagozzi, R. P. (2011). Measurement and meaning in information systems and organizational research: Methodological and philosophical foundations. *MIS Quarterly, 35*(2), 261-292.

Bagozzi, R. P., Gopinath, M., and Nyer, P. U. (1999). The role of emotions in marketing. *Journal of the Academy of Marketing Science, 27*(2), 184-206.

Bagozzi, R. P. and Yi, Y. (2012). Specification, evaluation, and interpretation of structural equation models. *Journal of the Academy of Marketing Science, 40*(1), 8-34.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191-215.

Bateman, T. S. and Organ, D. W. (1983). Job satisfaction and the good soldier: The relationship between affect and employee 'citizenship'. *Academy of Management Journal, 26*(4), 587-595.

Beck, K. H. (1984). The effects of risk probability, outcome severity, efficacy of protection and access to protection on decision making: A further test of protection motivation theory. *Social Behavior and Personality, 12*(2), 121-125.

Beer, G. (1980). The Cobb-Douglas production function. *Mathematics Magazine, 53*(1), 44-48.

Bennett, R. J. and Robinson, S. L. (2000). Development of a measure of workplace deviance. *Journal of Applied Psychology, 85*(3), 349-360.

Bennett, R. J. and Robinson, S. L. (2003). The past, present, and future of workplace deviance research. In J. Greenberg (Ed.), *Organizational Behavior: The State of the Science (2nd ed.)* (pp. 247-281). Mahwah, NJ: Lawrence Erlbaum.

Block, L. G. and Keller, P. A. (1995). When to accentuate the negative: The effects of perceived efficacy and message framing on intentions to perform a health-related behavior. *Journal of Marketing Research, 32*(2), 192-203.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective behaviors in users. *MIS Quarterly, 39*(In press).

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J., and Courtney, J. F. (2015). *Assessing the Role of Security Education, Training, and Awareness on Insiders' Security-related Behavior: An Expectancy Theory Approach.* Paper presented at the 48th Annual Hawaii International Conference on System Sciences (HICSS)

Carver, C. S. and Scheier, M. F. (1982). Control theory: A useful conceptual framework for personality–social, clinical, and health psychology. *Psychological Bulletin, 92*(1), 111-135.

Chadwick, I. C. and Raver, J. L. (2013, August 9-13). *Continuously improving in tough times: Overcoming resource constraints with psychological capital.* Paper presented at the Annual Meeting of the Academy of Management, Orlando, FL.

Chen, G., Gully, S. M., Whiteman, J.-A., and Kilcullen, R. N. (2000). Examination of relationships among trait-like individual differences, state-like individual differences, and learning performance. *Journal of Applied Psychology*, *85*(6), 835-847.

Cheung, F., Tang, C. S.-k., and Tang, S. (2011). Psychological capital as a moderator between emotional labor, burnout, and job satisfaction among school teachers in China. *International Journal of Stress Management, 18*(4), 348.

Chin, W. W., Thatcher, J. B., and Wright, R. T. (2012). Assessing common method bias: Problems with the ULMC technique. *MIS Quarterly, 36*(3), 1003-1019.

Cisco (2013). 2013 Cisco annual security report. Retrieved from http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2013_ASR.pdf

Cohen, J. (1992). A power primer. *Psychological Bulletin*, *112*(1), 155.

Conner, M. and Godin, G. (2007). Temporal stability of behavioural intention as a moderator of intention–health behaviour relationships. *Psychology and Health*, *22*(8), 875-897.

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior*, *28*(5), 1849-1858.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*(February), 90-101.

Culbertson, S. S., Fullagar, C. J., and Mills, M. J. (2010). Feeling good and doing great: The relationship between psychological capital and well-being. *Journal of Occupational Health Psychology, 15*(4), 421-433.

D'Arcy, J., Herath, T., and Shoss, M. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems, 31*(2), 285-318.

D'Arcy, J. and Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM, 50*(10), 113-117.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319-340.

Deci, E. L. (1972). Intrinsic motivation, extrinsic reinforcement, and inequity. *Journal of Personality and Social Psychology*, *22*(1), 113-120.

Diener, C. I. and Dweck, C. S. (1980). An analysis of learned helplessness: II. The processing of success. *Journal of Personality and Social Psychology*, *39*(5), 940-952.

Floyd, D. L., Prentice-Dunn, S., and Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407-429.

Folkman, S., Lazarus, R. S., Dunkel-Schetter, C., DeLongis, A., and Gruen, R. J. (1986). Dynamics of a stressful encounter: Cognitive appraisal, coping, and encounter outcomes. *Journal of Personality and Social Psychology*, *50*(5), 992-1003.

Fredrickson, B. L. (2001). The role of positive emotions in positive psychology: The broaden-and-build theory of positive emotions. *American Psychologist*, *56*(3), 218-226.

Fruin, D. J., Pratt, C., and Owen, N. (1992). Protection motivation theory and adolescents' perceptions of exercise. *Journal of Applied Social Psychology*, *22*(1), 55-69.

Fugate, M., Prussia, G. E., and Kinicki, A. J. (2012). Managing employee withdrawal during organizational change: The role of threat appraisal. *Journal of Management*, *38*(3), 890-914.

Gable, S. L. and Haidt, J. (2005). What (and why) is positive psychology? *Review of General Psychology*, *9*(2), 103-110.

Gefen, D., Straub, D. W., and Rigdon, E. E. (2011). An update and extension to SEM guidelines for administrative and social science research. *MIS Quarterly, 35*(2), iii-xiv.

Gerbing, D. W. and Anderson, J. C. (1988). An updated paradigm for scale development incorporating unidimensionality and its assessment. *Journal of Marketing Research, 25*(2), 186-192.

Goldberg, L. R. (1990). An alternative 'description of personality': The Big-Five factor structure. *Journal of Personality and Social Psychology, 59*(6), 1216-1229.

Gurung, A., Luo, X., and Liao, Q. (2009). Consumer motivations in taking action against spyware: An empirical investigation. *Information Management and Computer Security, 17*(3), 276-289.

Hair, J., Black, W., Babin, B., Anderson, R., and Tatham, R. (2006). *Multivariate Data Analysis* (6th ed.). Upper Saddle River, NJ: Prentice Hall.

Hair, J. F., Hult, G. T. M., Ringle, C. M., and Sarstedt, M. (2014). *A Primer on Partial Least Squares Structural Equations Modeling (PLS-SEM)*. Los Angeles, CA: Sage Publications.

Herath, T. and Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Hobfoll, S. E. (1989). Conservation of resources: A new attempt at conceptualizing stress. *American Psychologist, 44*(3), 513-524.

Hobfoll, S. E. (2002). Social and psychological resources and adaptation. *Review of General Psychology, 6*(4), 307-324.

Hsu, J., Shih, S.-P., Hung, Y. W., and Lowry, P. B. (2015). How extra-role behaviors can improve information security policy effectiveness. *Information Systems Research, 26*(2), 282-300.

Hu, L. and Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal, 6*(1), 1-55.

Huettner, D. A. and Costanza, R. (1982). Economic values and embodied energy. *Science, 216*(4550), 1141-1143.

Jarvis, C. B., MacKenzie, S. B., and Podsakoff, P. M. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of Consumer Research, 30*(2), 199-218.

Johnston, A. C. and Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549-566.

Judge, T. A. and Bono, J. E. (2001). Relationship of core self-evaluations traits—self-esteem, generalized self-efficacy, locus of control, and emotional stability—with job satisfaction and job performance: A meta-analysis. *Journal of Applied Psychology, 86*(1), 80-92.

Junglas, I. A., Johnson, N. A., and Spitzmuller, C. (2008). Personality traits and concern for privacy: An empirical study in the context of location-based services. *European Journal of Information Systems, 17*(4), 387-402.

LaRose, R., Rifon, N. J., and Enbody, R. (2008). Promoting personal responsibility for Internet safety. *Communications of the ACM, 51*(3), 71-76.

Lee, Y. and Kozar, K. A. (2008). An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. *Information & Management, 45*(2), 109-119.

Lee, Y. and Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177-187.

Leventhal, H. (1970). Findings and theory in the study of fear communications. *Advances in Experimental Social Psychology, 5*(1970), 119-186.

Liang, H., Saraf, N., Hu, Q., and Xue, Y. (2007). Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quarterly, 31*(1), 59-87.

Liang, H. and Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394-413.

Lowry, P. B. and Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies.

Information Systems Journal, *25*(5), 433-463.

Lowry, P. B., Moody, G. D., Galletta, D. F., and Vance, A. (2013). The drivers in the use of online whistle-blowing reporting systems. *Journal of Management Information Systems, 30*(1), 153-189.

Lowry, P. B., Posey, C., Bennett, R. J., and Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal, 25*(3), 193-230.

Lowry, P. B., Posey, C., Roberts, T. L., and Bennett, R. J. (2014). Is your banker leaking your personal information? The roles of ethics and individual-level cultural characteristics in predicting organizational computer abuse. *Journal of Business Ethics, 121*(3), 385-401.

Luthans, F. (2002). The need for and meaning of positive organizational behavior. *Journal of Organizational Behavior*, *23*(6), 695-706.

Luthans, F., Avey, J. B., Avolio, B. J., Norman, S. M., and Combs, G. M. (2006a). Psychological capital development: Toward a micro intervention. *Journal of Organizational Behavior, 27*(3), 387-393.

Luthans, F., Avey, J. B., and Patera, J. L. (2008a). Experimental analysis of a web-based training intervention to develop positive psychological capital. *Academy of Management Learning & Education, 7*(2), 209-221.

Luthans, F., Avolio, B. J., Avey, J. B., and Norman, S. M. (2007a). Positive psychological capital: Measurement and relationship with performance and satisfaction. *Personnel Psychology, 60*(3), 541-572.

Luthans, F., Norman, S. M., Avolio, B. J., and Avey, J. B. (2008b). The mediating role of psychological capital in the supportive organizational climate—employee performance relationship. *Journal of Organizational Behavior*, *29*(2), 219-238.

Luthans, F., Vogelgesang, G. R., and Lester, P. B. (2006b). Developing the psychological capital of resiliency. *Human Resource Development Review, 5*(1), 25-44.

Luthans, F., Youssef, C. M., and Avolio, B. J. (2007b). *Psychological Capital: Developing the Human Competitive Edge*. New York, NY: Oxford University Press.

MacKinnon, D. P., Lockwood, C. M., and Williams, J. (2004). Confidence Limits for the Indirect Effect: Distribution of the Product and Resampling Methods. *Multivariate behavioral research, 39*(1), 99-99.

Maddux, J. E. and Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469-479.

Milne, S., Sheeran, P., and Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology, 30*(1), 106-143.

Moore, A. P., Hanley, M., and Mundie, D. (2012). A pattern for increased monitoring for intellectual property theft by departing insiders. 1-17. Retrieved from http://repository.cmu.edu/sei/701/

Muthén, L. and Muthén, B. (1998-2010). Mplus User's Guide

Nabi, R. L., Roskos-Ewoldsen, D., and Carpentier, F. D. (2008). Subjective knowledge and fear appeal effectiveness: Implications for message design. *Health Communication, 23*(2), 191-201.

Nunnally, J. C. (1978). *Psychometric Theory*. New York, NY: McGraw-Hill.

Pahnila, S., Siponen, M., and Mahmood, A. (2007). *Employees' behavior towards IS security policy compliance.* Paper presented at the 40th Annual Hawaii International Conference on System Sciences (HICSS)

Parker, S. K. (1998). Enhancing role breadth self-efficacy: The roles of job enrichment and other organizational interventions. *Journal of Applied Psychology, 83*(6), 835-852.

Peters, G.-J. Y., Ruiter, R. A., and Kok, G. (2013). Threatening communication: A critical re-analysis and a revised meta-analytic test of fear appeal theory. *Health Psychology Review, 7*(Supplement 1), S8-S31.

Peterson, S. (2012). Leaders, cheer up! Positive thinking can boost organizational performance [Online Interview]. Retrieved from http://research.wpcarey.asu.edu/management-entrepreneurship/leaders-cheer-up-positive-thinking-can-boost-organizational-performance/

Peterson, S., Luthans, F., Avolio, B. J., Walumbwa, F. O., and Zhang, Z. (2011). Psychological capital and employee performance: A latent growth modeling approach. *Personnel Psychology, 64*(2), 427-450.

Petter, S., Straub, D. W., and Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly, 31*(4), 623-656.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., and Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879-903.

Posey, C., Roberts, T., Lowry, P. B., Bennett, R. J., and Courtney, J. F. (2010, October 8-9). *Insiders' protection of organizational information assets: A multidimensional scaling study of protection-motivated behaviors.* Paper presented at the The Dewald Roode Information Security Workshop 2010, Waltham, MA.

Posey, C., Roberts, T. L., and Lowry, P. B. (2015a). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179-214.

Posey, C., Roberts, T. L., Lowry, P. B., and Bennett, R. J. (2015b). Multiple indicators and multiple causes (MIMIC) models as a mixed-modelling technique: A tutorial and an annotated example. *Communications of the Association for Information Systems, 36*(1), article 11.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., and Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly, 37*(4), 1189-1210.

Richardson, H. A., Simmering, M. J., and Sturman, M. C. (2009). A tale of three perspectives. *Organizational Research Methods, 12*(4), 762-800.

Rippetoe, P. A. and Rogers, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology, 52*(3), 596-604.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93-114.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social Psychophysiology: A Sourcebook* (pp. 153-176). New York, NY: Guilford.

Rogers, R. W. and Prentice-Dunn, S. (1997). Protection motivation theory *Handbook of Health Behavior Research I: Personal and Social Determinants* (Vol. xxvii, pp. 113-132). New York, NY: Plenum Press.

Scheier, M. F. and Carver, C. S. (1985). Optimism, coping, and health: Assessment and implications of generalized outcome expectancies. *Health Psychology, 4*(3), 219-247.

Seligman, M. and Csikszentmihalyi, M. (2000). Positive psychology: An introduction. *American Psychologist, 55*(1), 5-14.

Sheldon, K. M. and King, L. (2001). Why positive psychology is necessary. *American Psychologist, 56*(3), 216-217.

Siponen, M., Mahmood, M. A., and Pahnila, S. (2009). Technical opinion: Are employees putting your company at risk by not following information security policies? *Communications of the ACM, 52*(12), 145-147.

Siponen, M., Pahnila, S., and Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *IEEE Computer, 43*(2), 64-71.

Siponen, M. and Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487-502.

Smith, W. K. and Lewis, M. W. (2011). Toward a theory of paradox: A dynamic equilibrium model of organizing. *Academy of Management Review, 36*(2), 381-403.

Snyder, C., Irving, L. M., and Anderson, J. R. (1991). Hope and health: Measuring the will and the ways. In C. R. Snyder & D. R. Forsyth (Eds.), *Handbook of Social and Clinical Psychology: The Health Perspective* (pp. 285-305). New York: Pergamon.

Snyder, C. R., Sympson, S. C., Ybasco, F. C., Borders, T. F., Babyak, M. A., and Higgins, R. L. (1996). Development and validation of the State Hope Scale. *Journal of Personality and Social Psychology, 70*(2), 321-335.

Stanton, J. M., Stam, K. R., Mastrangelo, P. M., and Jolton, J. A. (2006). Behavioral information security: An overview, results, and research agenda. In P. Zhang & D. F. Galletta (Eds.), *Human-Computer Interaction and Management Information Systems: Foundations* (pp. 262-280). Armonk, NY: M.E. Sharpe.

Straub, D., Boudreau, M. C., and Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems, 13*(24), 380-427.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly, 13*(2), 147-169.

Tanner, J. F., Day, E., and Crask, M. R. (1989). Protection motivation theory: An extension of fear appeals theory in communication. *Journal of Business Research, 19*(4), 267-276.

Vance, A., Lowry, P. B., and Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems, 29*(4), 263-289.

Vance, A., Lowry, P. B., and Eggett, D. (2015). A new approach to the problem of access policy violations: Increasing perceptions of accountability through the user interface. *MIS Quarterly, 39*(2), 345-366.

Vroom, V. (1964). *Work and Motivation*. Oxford, UK: Wiley.

Wagnild, G. M. and Young, H. M. (1993). Development and psychometric evaluation of the Resilience Scale. *Journal of Nursing Measurement, 1*(2), 165-178.

Wang, Y., Liu, L., Wang, J., and Wang, L. (2012). Work-family conflict and burnout among Chinese doctors: The mediating role of psychological capital. *Journal of Occupational Health, 54*(3), 232-240.

Warkentin, M., Johnston, A. C., Walden, E., and Straub, D. W. (2016). Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Examination. *Journal of the Association for Information Systems, 17*(3), 194-215.

Welbourne, T. M. and Felton, R. W. (1998). Improving technology-based change processes: A case study of Indus International. *Journal of Strategic Performance Measurement, 2*(2), 22-25.

West, S. G., Finch, J. F., and Curran, P. J. (1995). Structural equation models with nonnormal variables: Problems and remedies. In Hoyle (Ed.), *Structural Equation Modeling: Concepts, Issues and Applications* (pp. 56-75). Newbury Park, CA: Sage.

Williams, L. J. and Anderson, S. E. (1991). Job satisfaction and organizational commitment as predictors of organizational citizenship and in-role behaviors. *Journal of Management, 17*(3), 601-617.

Williams, L. J., Hartman, N., and Cavazotte, F. (2010). Method variance and marker variables: A review and comprehensive CFA marker technique. *Organizational Research Methods, 13*(3), 477-514.

Willison, R. and Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1-20.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs, 59*(4), 329-349.

Witte, K. (1994). Fear control and danger control: A test of the extended parallel process model (EPPM). *Communications Monographs, 61*(2), 113-134.

Witte, K. and Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior, 27*(5), 591-615.

Witte, K., Cameron, A., McKeon, J. K., and Berkowitz, J. M. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication, 1*(4), 317-342.

Woon, I., Tan, G. W., and Low, R. (2005). *A protection motivation theory approach to home wireless security*. Paper presented at the International Conference on Information Systems (ICIS).

Workman, M., Bommer, W. H., and Straub, D. W. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799-2816.

Zafar, H. and Clark, J. G. (2009). Current state of information security research in IS. *Communications of the Association for Information Systems, 24*(1), 557-596.

Zuckerman, M. (1983). The distinction between trait and state scales is not arbitrary: Comment on Allen and Potkay's 'On the arbitrary distinction between traits and state'. *Journal of Personality and Social Psychology, 44*(5), 1083-1086.

Table 1. Initial Measurement Model Statistics

Latent Construct	M	SD	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)
(1) Self-efficacy[t]	5.29	1.17	0.90													
(2) Optimism[t]	4.91	1.14	0.80	0.84												
(3) Resilience[t]	5.51	0.92	0.86	0.84	0.80											
(4) Hope[t]	5.35	1.00	0.88	0.85	0.93	0.88										
(5) Fear	2.03	1.25	-0.21	-0.21	-0.23	-0.23	0.95									
(6) Threat severity	3.37	1.54	-0.14	-0.14	-0.15	-0.15	0.34	0.91								
(7) Threat Vulnerability	3.41	1.51	-0.17	-0.16	-0.17	-0.18	0.34	0.79[a]	0.92							
(8) Security response efficacy	5.36	1.14	0.45	0.44	0.48	0.49	-0.23	-0.12	-0.24	0.87						
(9) Response cost	2.68	1.37	-0.29	-0.28	-0.31	-0.31	0.32	0.26	0.32	-0.53	0.89					
(10) Security self-efficacy	5.25	1.16	0.44	0.43	0.47	0.47	-0.18	-0.05	-0.12	0.95[b]	-0.54	0.83				
(11) Maladaptive rewards	1.95	1.29	-0.18	-0.17	-0.19	-0.19	0.29	0.36	0.35	-0.23	0.55	-0.20	0.92			
(12) Protection motivation	5.61	1.26	0.43	0.42	0.45	0.46	-0.19	-0.04	-0.11	0.71	-0.58	0.73	-0.37	0.78		
(13) PMBs	4.94	1.74	0.19	0.19	0.21	0.21	0.13	0.16	0.07	0.47	-0.29	0.56	-0.06	0.60	0.96	
(14) PsyCap	5.26	0.95	0.90	0.88	0.96	0.97	-0.24	-0.15	-0.18	0.50	-0.32	0.49	-0.20	0.48	0.21	0.96

Estimator: MLR Chi-Square = 2347.289 DF=1490; Scaling Correction Factor for MLR = 1.1157; CFI=0.937; TLI=0.932; RMSEA=0.039; SRMR=0.048

[t] PsyCap Subconstructs

[a] High correlation between threat severity and threat vulnerability

[b] Security self-efficacy and security response efficacy failed Fornell-Larcker criterion.

Composite reliabilities shown on diagonal.

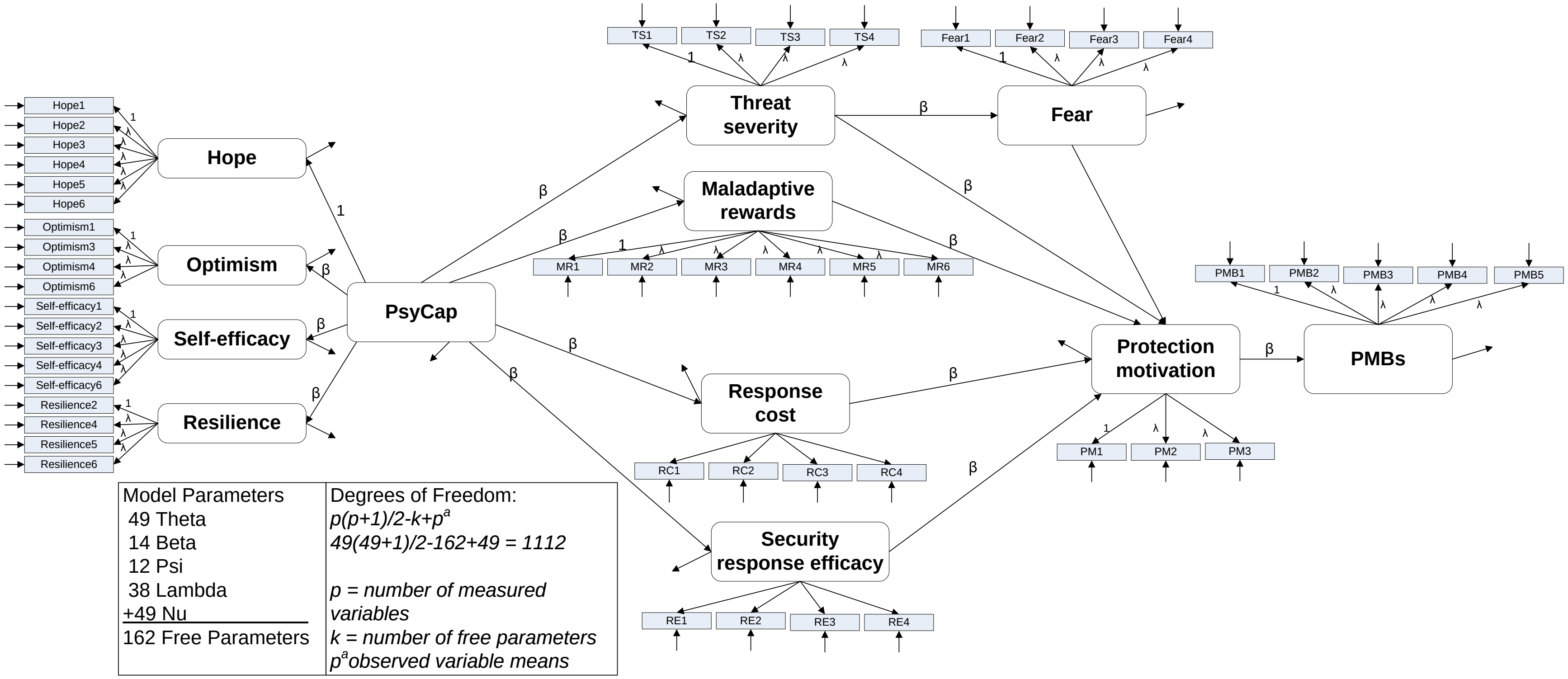
Table 2. Refined Measurement Model Statistics

Latent Construct	M	SD	(1)	(2)	(3)	(4)	(5)	(6)	(8)	(9)	(10)	(11)	(12)	(13)
(1) Self-efficacy[t]	5.29	1.17	0.90											
(2) Optimism[t]	4.91	1.14	0.80	0.84										
(3) Resilience[t]	5.51	0.92	0.86	0.84	0.80									
(4) Hope[t]	5.35	1.00	0.88	0.85	0.93	0.88								
(5) Fear	2.03	1.25	-0.21	-0.21	-0.23	-0.23	0.95							
(6) Threat severity	3.37	1.54	-0.14	-0.14	-0.15	-0.15	0.34	0.91						
(8) Security response efficacy	5.36	1.14	0.45	0.44	0.48	0.48	-0.23	-0.13	0.87					
(9) Response cost	2.68	1.37	-0.29	-0.28	-0.31	-0.31	0.32	0.27	-0.53	0.89				
(10) Maladaptive rewards	1.95	1.29	-0.18	-0.17	-0.19	-0.19	0.29	0.36	-0.23	0.55	0.92			
(11) Protection motivation	5.61	1.26	0.43	0.42	0.45	0.46	-0.19	-0.04	0.70	-0.58	-0.37	0.78		
(12) PMBs	4.94	1.74	0.19	0.19	0.21	0.21	0.13	0.16	0.47	-0.29	-0.06	0.60	0.96	
(13) PsyCap	5.26	0.95	0.90	0.88	0.96	0.97	-0.24	-0.16	0.50	-0.32	-0.20	0.48	0.21	0.96

Estimator: MLR Chi-Square = 1680.968 DF=1095; Scaling Correction Factor for MLR = 1.1231; CFI=0.947 TLI =0.944; RMSEA=0.038; SRMR=0.048

[t] PsyCap Subconstructs

Composite reliabilities shown on diagonal.



Model Parameters	Degrees of Freedom:
49 Theta	$p(p+1)/2-k+p^a$
14 Beta	*49(49+1)/2-162+49 = 1112*
12 Psi	
38 Lambda	*p = number of measured*
+49 Nu	*variables*
162 Free Parameters	*k = number of free parameters*
	p^a*observed variable means*

Figure 1. Empirical Model: Measurement and Structural Components

Appendix A. Measurement details

Table 3. Study Measures

Measures (Citations)	**Prompts and Measurement Items**	**Mean**	**Std.**
PsyCap hope[i] (Luthans et al., 2007a)	Instructions: ”Please indicate your level of agreement with the following statements:”		
	PCH-1. If I should find myself in a jam at work, I could think of many ways to get out of it.	5.30	1.24
	PCH-2. At the present time, I am energetically pursuing my work goals.	5.12	1.40
	PCH-3. There are lots of ways around any problem.	5.42	1.21
	PCH-4. Right now I see myself as being pretty successful at work.	5.50	1.27
	PCH-5. I can think of many ways to reach my current work goals.	5.30	1.21
	PCH-6. At this time, I am meeting the work goals that I set for myself.	5.44	1.23
PsyCap resilience (Luthans et al., 2007a)	Instructions: ”Please indicate your level of agreement with the following statements:”		
	PCR-2. I usually manage difficulties one way or another at work.	5.65	1.02
	PCR-4. I usually take stressful things at work in stride.	5.15	1.31
	PCR-5. I can get through difficult times at work because I’ve experienced difficulty before.	5.56	1.21
	PCR-6. I feel I can handle many things at a time at this job.	5.71	1.15
PsyCap optimism[i] (Luthans et al., 2007a)	Instructions: “Please indicate your level of agreement with the following statements:”		
	PCO-1. When things are uncertain for me at work, I usually expect the best.	4.64	1.40
	PCO-3. I always look on the bright side of things regarding my job.	5.17	1.31
	PCO-4. I’m optimistic about what will happen to me in the future as it pertains to work.	4.96	1.52
	PCO-6. I approach this job as if ‘every cloud has a silver lining’.	4.85	1.35
PsyCap self-efficacy[i] (Luthans et al., 2007a)	Instructions: “Please indicate your level of agreement with the following statements:”		
	PCSE-1. I feel confident analyzing a long-term problem to find a solution.	5.34	1.30
	PCSE-2. I feel confident in representing my work area in meetings with management.	5.38	1.39
	PCSE-3. I feel confident contributing to discussions about the company’s strategy.	5.04	1.44
	PCSE-4. I feel confident helping to set targets/goals in my work area.	5.31	1.29
	PCSE-6. I feel confident presenting information to a group of colleagues.	5.36	1.50
Fear[ii] (Block & Keller, 1995)	Instructions: “When thinking about the security threats to your organization’s information and information systems, to what extent do you feel...”		
	Fear-1. Frightened	1.84	1.25
	Fear-2. Nervous	2.05	1.36
	Fear-3. Anxious	2.12	1.39
	Fear-4. Uncomfortable	2.11	1.36
Threat vulnerability[i] (Workman et al., 2008)	Instructions: “Please indicate your level of agreement with the following statements about information security threats to your organization:”		
	TV-1. My organization’s information and information systems are vulnerable to security threats.	3.34	1.65
	TV-2. It is likely that an information security violation will occur to my organization’s information and information systems.	3.36	1.68
	TV-3. My organization’s information and information systems are at risk to information security threats.	3.43	1.69
	TV-4. My organization’s information and information systems are	3.50	1.66

Measures (Citations)	Prompts and Measurement Items	Mean	Std.
	susceptible to information security threats.		
Threat severity[i] (Workman et al., 2008)	Instructions: "Please indicate your level of agreement with the following statements about information security threats to your organization:"		
	TS-1. Threats to the security of my organization's information and information systems are severe.	3.17	1.70
	TS-2. In terms of information security violations, attacks on my organization's information and information systems are severe.	2.98	1.64
	TS-3. I believe that threats to the security of my organization's information and information systems are serious.	3.81	1.85
	TS-4. I believe that threats to the security of my organization's information and information systems are significant.	3.54	1.77
Security response efficacy[i] (Workman et al., 2008)	Instructions: "Please indicate your level of agreement with the following statements about yourself and information security threats to your organization:"		
	RE-1. Employee efforts to keep my organization's information and information systems safe from information security threats are effective.	5.34	1.28
	RE-2. The available measures that can be taken by employees to protect my organization's information and information systems from security violations are effective.	5.37	1.32
	RE-3. The preventive measures available to me to stop people from accessing my organization's information and information systems are adequate.	5.32	1.32
	RE-4. If I perform the preventive measures available to me, my organization's information and information systems are less likely to be exposed to a security threat.	5.43	1.46
Security self-efficacy[i] (Workman et al., 2008)	Instructions: "Please indicate your level of agreement with the following statements about yourself and the information security threats to your organization:"		
	SSE-1. For me, taking information security precautions to protect my organization's information and information systems is easy.	5.38	1.30
	SSE-2. I have the necessary skills to protect my organization's information and information systems from information security violations.	5.06	1.53
	SSE-3. My skills required to stop information security violations against my organization's information and information systems are adequate.	5.14	1.46
	SSE-4. I believe that I could learn to perform the preventive measures to protect my organization's information and information systems effectively.	5.43	1.40
Response cost[i] (Workman et al., 2008)	Instructions: "Please indicate your level of agreement with the following statements about yourself and information security threats to your organization:"		
	RC-1. The inconvenience of implementing recommended security measures to protect my organization's information and information systems exceeds the potential benefits.	2.89	1.68
	RC-2. The negative impact on my work from recommended security measures to protect my organization's information and information systems is greater than the benefits gained from the security measures.	2.80	1.56
	RC-3. Recommended security measures are so much of a nuisance that I think my organization would be better without them.	2.41	1.55
	RC-5. The negative side effects of recommended security measures in my organization are greater than the advantages.	2.62	1.56

Measures (Citations)	**Prompts and Measurement Items**	**Mean**	**Std.**
Maladaptive rewards[i] (Posey et al., 2015a)	Instructions: "Please indicate your level of agreement with the following statements about information security threats to your organization:" NOTE: Rewards in these statements refer to ANY personal rewards that you could receive from ANY organization, institution, or individual, including yourself.		
	MR-1. It is likely that I would receive personal rewards for purposefully not protecting my organization's information and information systems from security threats.	1.93	1.52
	MR-2. I could be rewarded personally for not protecting my organization from information security threats.	1.95	1.55
	MR-3. I would receive personal gratification for purposefully not protecting my organization from its information security threats.	1.76	1.39
	MR-4. I would feel a sense of internal satisfaction for allowing information security threats to harm my organization.	1.85	1.51
	MR-5. I could be rewarded financially for choosing not to protect my organization's information and information systems from security threats.	2.03	1.61
	MR-6. I believe others would be willing to reward me financially for intentionally failing to protect my organization's information and information systems from security threats.	2.19	1.69
Protection motivation[i] (Posey et al., 2015a)	Instructions: "Please indicate your level of agreement with the following statements about information security threats to your organization:"		
	PM-1. I intend to protect my organization from its information security threats.	5.90	1.26
	PM-2. My intentions to prevent my organization's information security threats from being successful are high.	5.58	1.53
	PM-3. It is likely that I will engage in activities that protect my organization's information and information systems from security threats.	5.66	1.52
	PM-4. I intend to expend effort to protect my organization from its information security threats.	5.29	1.79
Protection-motivated behaviors[iii] (Posey et al., 2015a)	Instructions:"Given the following statements, on what basis did you engage in the stated behaviors in the last year?:"		
	PMB-1. I actively attempted to protect my organization's information and computerized information systems.	5.00	1.87
	PMB-2. I tried to safeguard my organization's information and information systems from information security threats.	5.09	1.79
	PMB-3. I took committed action to prevent information security threats to my firm's information and computer systems from being successful.	4.72	1.95
	PMB-4. I purposefully defended my organization from information security threats to its information and computerized information systems.	4.76	1.93
	PMB-5. I earnestly attempted to keep my organization's information and computer systems from harm produced by information security threats.	5.12	1.84

Note: Scaling was as follows: [i] 1 = Strongly disagree to 7 Strongly agree; [ii] 1 Not at all to 7 Very large extent; [iii] 1 Never to 7 Always

Appendix B. Supplement on Common-Method Variance

According to a recent analysis of common-method variance (CMV) detection and correction techniques in IS, the most frequent technique has been the unmeasured latent method construct (ULMC) technique. However, that technique has serious shortcomings in both detecting and correcting CMV (Chin et al., 2012). The CFA marker-variable technique, however, has been found to accurately and consistently detect CMV (Richardson et al., 2009) and is relatively underused in IS (Chin et al., 2012, p. A2). This method is particularly well suited for CB-SEM because, unlike ULMC, it specifies the comparison of free and restrained models in such a way that allows for appropriate model identification (Liang et al., 2007; Williams et al., 2010). The CFA marker-variable technique tests for CMV, unequal (congeneric) method variance, and bias due to CMV. The analysis essentially compares the fit of three competing CFA results that have varying constraints imposed.

According to methodologists, the unmeasured latent method factor has three advantages: (1) "it does not require the researcher to identify and measure the specific factor responsible for the method effects;" (2) it "models the effect of the method factor on the measures rather than on the latent constructs they represent;" and (3) it "does not require the effects of the method factor on each method to be equal" (Petter et al., 2007, p. 894). It is important to note that the CFA marker-variable technique shares these advantages while remaining fully identified. For this research, we chose a marker variable that measures attitude toward the color blue. The three items chosen were: (1) I prefer blue to other colors, (2) I like the color blue, and (3) I like blue clothes (Cronbach's α = 0.840.).

As previous literature describes, to conduct the full test, we ran five CFAs (Richardson et al., 2009; Williams et al., 2010):

1. A totally free model (Figure 4)
2. A baseline model that restrains the correlations between the substantive items and the marker variable to zero and constrains the loadings of the marker items onto the marker variable and the marker-variable error terms to the unstandardized results from the totally free model (Figure 5)
3. A method-C model that is the same as the baseline except that it constrains the factor loadings from the marker variable to each substantive item to be equal to one another (Figure 6)
4. A method-U model that, again, is the same as the method-C model, except that the factor loadings from the marker variable to the substantive items are no longer constrained to be equal (Figure 7)
5. A method-R model that is the same as either C or U (depending on which exhibited better fit), except that the correlations among the substantive variables are constrained to the unstandardized correlations from the baseline model (Figure 8 and Figure 9)

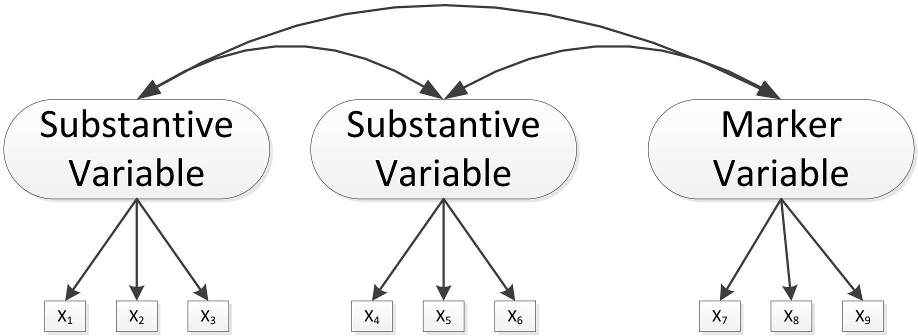


Figure 2. CFA 1: Totally Free CFA

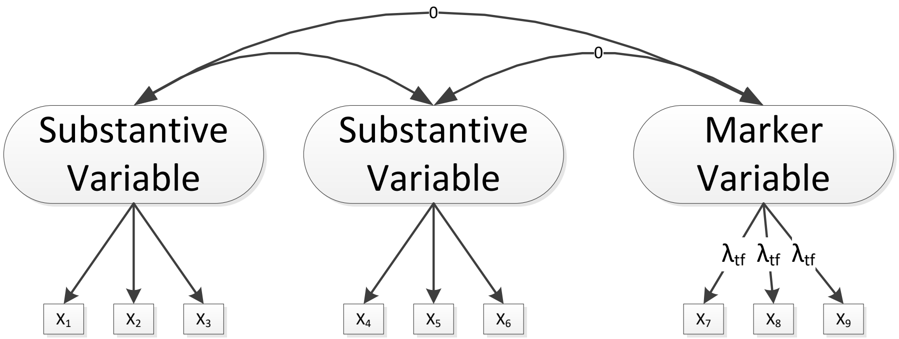
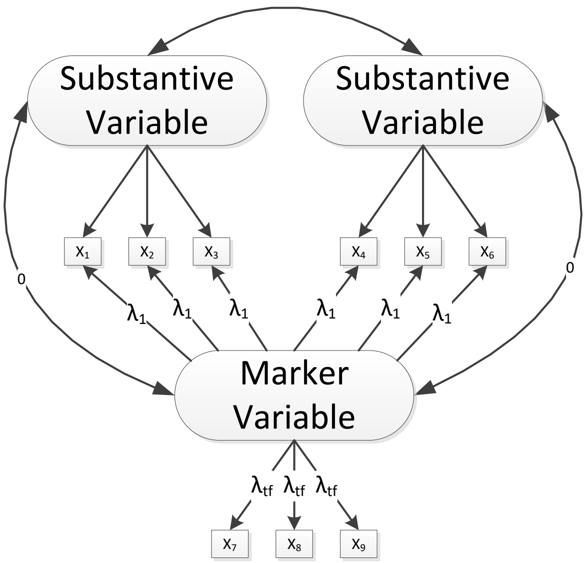


Figure 3. CFA 2: Baseline Model


Substantive Variable
Substantive Variable
X_1
X_2
X_3
X_4
X_5
X_6
0
0
λ_1 λ_1 λ_1 λ_1 λ_1 λ_1
Marker Variable
λ_{tf} λ_{tf} λ_{tf}
X_7
X_8
X_9

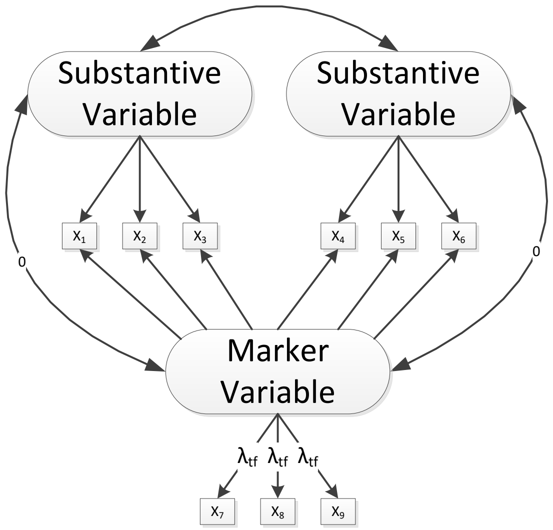
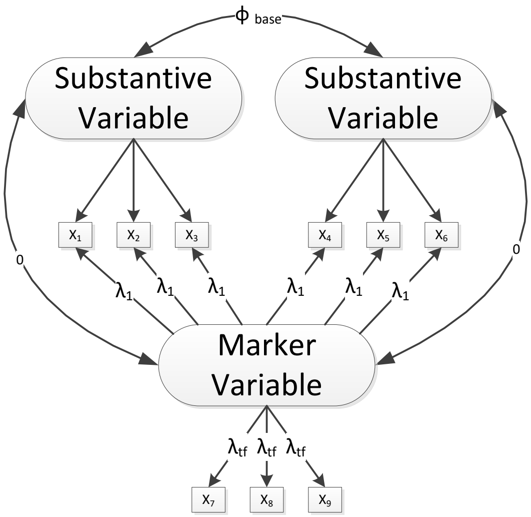


Figure 4. CFA 3: Method-C Model

Figure 5. CFA 4: Method-U Model



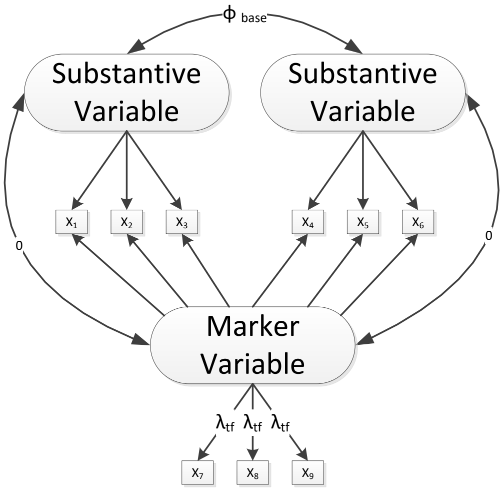


Figure 6. Method-R Model (Based on Method-C)

Figure 7. Method-R Model (Based on Method-U)

To test for CMV, we tested the fit of the CFAs modelled above for significant differences. Specifically, we tested the following models for significant differences:

1. We tested the baseline model for significantly different fit from the method-C model. If method-C had significantly better fit, it indicated CMV.
2. We tested the method-C model fit for significantly different fit from the method-U model. If method-U had better fit, there was evidence of unequal method effects.
3. We tested the method-R model fit for significantly different fit from the method-C or method-U model (whichever exhibited better fit). If method-R fit worse than method-C or method-U, there was evidence of bias due to CMV.

To assess the implications of CMV in our sample, we included four variables in our marker-variable technique: three substantive variables and our marker variable. We included a substantive variable from each appraisal (i.e., *fear* from the threat appraisal and *response cost* from the coping appraisal) and our dependent variable (*PMBs*).The results of the CFA marker-variable technique indicate that CMV is not an issue for the current study. The results appear in Table 8.

Table 4. CFA Marker-Variable Results

Model	**Model Fit**	**Model Comparison**	**CFI**	**Result**

Baseline Model	X2 = 137.604
	d.f. = 107
			0.994	

Method-C Model	X2 = 137.502
	d.f. = 106
		Baseline vs. Method-C
		ΔX2 = 0.102; d.f. = 1; (p = 0.749)
			0.994	No CMV detected

Method-U Model	X2 = 128.697
	d.f. = 94
		Method-C vs. Method-U
		ΔX2 = 6.805; d.f. = 12 (p = 0.870)
			0.993	No unequal method effects detected

Method-R (Base-U)	X2 = 128.723
	d.f. = 97
		Method-U vs. Method-R
		ΔX2 = 0.026; d.f. = 3 (p = 0.999)
			0.994	No bias from CMV detected

Method-R (Base-C)	X2 = 137.503
	d.f. = 109
		Method-C vs. Method-R
		ΔX2 = 0.001; d.f. = 3 (p = 0.999)
			0.995	No bias from CMV detected

Appendix C. Post Hoc Exploration of PsyCap

We assessed the level of protection motivation and PMBs for insiders with relatively high and relatively low levels of PsyCap (Table 9 and Figure 10).To examine whether higher-PsyCap individuals perform PMBs at a higher level than lower-PsyCap insiders, we performed an independent samples t-test in SPSS (v. 22), grouping insiders with PsyCap above the median level as higher-PsyCap and those below (inclusive) the median level as lower-PsyCap. As in our CMV analysis, we included a theoretically unrelated construct to ensure that any differences we found for protection motivation and/or PMBs across PsyCap levels were not due to some methodological artifact (e.g., groups reporting statistically higher or lower scores in general). Our results (which appear in Table 9 and Figure 10) demonstrate that the mean PMB and protection motivation are greater for those insiders with relatively high PsyCap and that there was no mean difference across groups for our theoretically unrelated construct.

Table 5. Mean Across PsyCap Levels

Construct	Mean	t-value (sig.)
PMBs[i]		
Lower PsyCap (n = 189)	4.75	2.117^{*}
Higher PsyCap (n = 188)	5.13	
Protection Motivation[i]		
Lower PsyCap (n = 189)	5.22	6.381^{***}
Higher PsyCap (n = 188)	6.01	
Blue Scale[i]		
Lower PsyCap (n = 189)	4.80	1.080
Higher PsyCap (n = 188)	4.94	

[i] Equal variances assumed (Levene's test insignificant at p = 0.05)

Median PsyCap level = 5.329

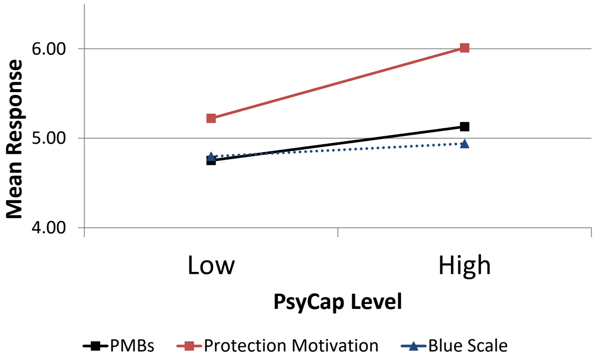


Figure 8. Differences Across PsyCap Levels