International Journal of Information Security and Privacy
Volume 20 • Issue 1 • January-December 2026

Integrating Psychological Ownership and Protection Motivation Theory in Chinese IT Organizations

Xiaofen Ma
http://orcid.org/0000-0003-0410-8206
Renmin University of China, China

Hichang Cho
National University of Singapore, Singapore
Received: October 23rd, 2025 | **Accepted:** April 6th, 2026

ABSTRACT

Protection motivation theory (PMT) has long explained information security behavior as a rational evaluation of threats and coping mechanisms. However, existing models provide limited insight into how organisational conditions translate into information security experts' personal responsibility for protecting information assets. This study addresses this gap by integrating psychological ownership (PO) into PMT and reconceptualising protection motivation as an ownership-driven process. Using survey data from 1,254 information security professionals in Chinese IT organisations and structural equation modelling, the results show that PO is the strongest predictor of protective intention. PO significantly strengthens threat appraisal and self-efficacy, whereas response efficacy and response cost do not significantly influence intention. These findings suggest that security behavior is driven less by calculative threat evaluation than by the internalisation of organisational responsibility, offering a psychologically grounded perspective on sustainable information security engagement.

KEYWORDS

Information Security, Psychological Ownership, Protection Motivation Theory, Organisational Commitment, Organisational Support

INTRODUCTION

Information technology (IT) organizations face increasing cybersecurity threats, and technological safeguards alone are no longer sufficient to ensure effective information security. As a result, scholars and practitioners have begun to recognize the importance of psychological factors in shaping employees' security behavior (Creemers, 2023; Ma & Cho, 2022). In particular, psychological ownership (PO) may play a critical role in motivating information security (IS) professionals to proactively safeguard organizational data assets. To build more resilient defenses, organizations must go beyond technical solutions and develop robust threat intelligence strategies that involve understanding not only external threat actors but also the motivations and behaviors of internal protectors (Ma, 2022).

Answering key questions, such as who protects organizational data, why they are motivated to do so, and how they act on that responsibility, is essential to anticipating and mitigating risk. One persistent and critical concern is the threat posed by insiders. Data leaks caused by IS professionals

DOI: 10.4018/IJISP.407403

with privileged access remain a serious issue (Li et al., 2019). These incidents underscore the need to better understand the psychological and organizational factors that influence insider behaviors. Ultimately, effective IS depends not only on technology but also on fostering a workforce that feels personally accountable for protecting the organization's digital assets.

As Simone Weil (1952) famously articulated, "A gardener, after a certain time, feels that the garden belongs to him [or her]" (p. 33). When IS professionals feel a psychological connection to the data they protect, their commitment extends beyond technical duties to fostering a proactive and resilient security culture. This sense of PO not only drives individual motivation but also strengthens the overall organizational defense against evolving digital risks. Equipped with the expertise to collect, analyze, and deploy data to implement technical solutions, these professionals are responsible for safeguarding organizational data and fortifying the organization's IS posture. A sense of ownership fosters perceived self-control, emotional attachment, and responsibility (Menard et al., 2018). Consequently, this sense of ownership applies to IS, where professionals are tasked with nurturing and protecting their organization's information systems.

This study aims to address three critical gaps identified in the existing IS literature. Although IS has long been framed as a technical issue, technical controls alone cannot prevent breaches. IS professionals must also exercise judgment, analyzing risks, drafting policies, and choosing safeguards to respond to violations. These supervisory tasks are vital for organizational security and success (Albrechtsen & Hovden, 2009). First, despite the extensive application of protection motivation theory (PMT) in IS research, existing models predominantly emphasize cognitive threat and coping appraisals while under-theorizing the motivational bridge between the organizational context and individual protective intention. Specifically, prior frameworks explain how individuals evaluate threats (Bekkers et al., 2023) but offer limited insight into why organizational antecedents translate into personally endorsed security behaviors. This study advances the literature by introducing PO as a proximal motivational mechanism that connects organizational conditions to individual security intentions. Unlike traditional PMT variables, which operate at the level of cognitive evaluation, PO captures a self-definitional attachment to organizational assets (Alshammari & Al-Mamary, 2026), thereby explaining how security-related behaviors become internalized rather than merely compliance-driven.

Second, IS research has predominantly focused on external motivators for understanding compliance with security policies within organizations. However, recent studies have highlighted the limitations of such approaches, which often rely on formal controls to enforce IS policies, such as rewards, monitoring, and sanctions. Imposing external controls over IS-related tasks may even provoke feelings of oppression among organizational members, exacerbating resistance to compliance efforts. By examining the concept of PO, we aim to shed light on how positive intrinsic motivations toward IS security are facilitated by IS professionals' sense of attachment and identification. Although several studies have examined the role of PO in the context of IS (e.g., Yoo et al., 2018), previous research has primarily focused on the direct relationship between PO and IS compliance or treated PO as a manipulated variable (e.g., Menard et al., 2018). While useful, these approaches may overlook the gradual and enduring processes, such as organizational support, emotional attachment, self-investment, and perceived control, all of which contribute to the formation and enactment of PO in real organizational settings. Therefore, the present study explores the antecedents and mediating mechanisms that underpin the relationship between PO and IS behavior, providing a deeper understanding of how PO influences IS protection in practice.

Third, despite China's unique cultural and institutional landscape and its rapidly expanding IT sector, there remains a significant gap in the research on IS protection within the country. In China's collectivist culture, where employees often exhibit strong identification with their organizational roles and teams (Hui et al., 2004), there is a clear need for studies examining the complexities of IS dynamics and their underlying sociopsychological processes.

Using PMT as a foundational theoretical framework, this study proposes a new model for IS protection, detailing the relationship between PO and the key PMT variables that affect protection