Feng Xu, Carol Hsu, David Wang, and Paul Benjamin Lowry (2023). "The antecedents of employees' proactive information security behavior: The perspective of proactive motivation," ***Information Systems Journal (ISJ)*** (accepted 06-Nov-2023).

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. Feng Xu**
  - College of Business, University of Michigan-Dearborn
  - Email: fengxu@umich.edu
  - Website: https://www.linkedin.com/in/feng-xu-57a3a3236/
- **Professor Carol Hsu**
  - Business Information Systems
  - The University of Sydney Business School, the University of Sydney
  - Email: carol.hsu@sydney.edu.au
  - Website: https://www.sydney.edu.au/business/about/our-people/academic-staff/carol-hsu.html
- **Professor Tawei (David) Wang**
  - School of Accounting & MIS, DePaul University, Chicago
  - Email: david.wang@depaul.edu
  - Website: https://business.depaul.edu/faculty/faculty-a-z/Pages/david-wang.aspx
- **Prof. Paul Benjamin Lowry,** Eminent Scholar and Suzanne Parker Thornhill Chair Professor
  - Business Information Technology, Pamplin College of Business
  - Virginia Tech
  - 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

The Antecedents of Employees' Proactive Information Security Behavior: The Perspective of Proactive Motivation

Abstract

Organizational information security (ISec) protection is undergoing a turbulent shift in the workplace environment. In an environment of ever-increasing risks of insider threats and external cyberattacks, individual employees are often expected to take the initiative to solve organizational security problems. This study therefore focuses on employees' proactive *information security behaviors* (ISBs)—behaviors that are self-initiated, change-oriented, and future-focused—and the motivations that compel employees to protect organizational assets. We ground our study in Parker et al.'s (2010) proactive motivation theory (ProMT) and develop an integrated multilevel model to examine the respective effects of proactive motivational states, that is, *can-do*, *reason-to*, and *energized-to* motivations, on employees' proactive ISBs. We also explore the roles of individual differences and contextual factors—namely, proactive personality and supervisory ISec support—and their influences on proactive motivational states. Data were collected from 210 employees situated in 55 departments distributed among multiple organizations located in China. The results show that supervisory ISec support positively influences employees' proactive motivational states and thereby boosts employees' proactive ISBs. Proactive personality negatively moderates the effect of supervisory ISec support on flexible security role orientation (reason-to motivation). By identifying the antecedents of employees' proactive ISBs, we make key theoretical contributions to ISec research and valuable practical contributions to organizational ISec management.

KEYWORDS

information security behaviors (ISBs), proactive ISBs, proactive motivation theory (ProMT), proactive motivational states, supervisory ISec support, proactive personality

1 INTRODUCTION

Today's global information security (ISec) environment is increasingly complex and dynamic due to the escalating risks of insider threats, deceptive threat actors, and newly emerging cyberattacks. For instance, the emerging hybrid work model has introduced new security vulnerabilities and new challenges for organizational data protection and access. *Organizational information security* refers to the practice of protecting sensitive information from unauthorized access, use, disclosure, disruption, modification, or destruction. It involves the implementation of measures and controls to ensure the confidentiality, integrity, and availability of information. Ever-evolving ransomware attacks—commonly distributed through phishing emails or text messages—require employees to be more vigilant and act as the first line of defense against threats such as zero-day attacks and breaches (IBM, 2022). In light of these growing threats, anecdotal evidence suggests that employees with a high level of autonomy and personal accountability play a highly valuable role in helping organizations manage these risks, mitigate dangers, and build robust cyber resilience (NCSAM, 2019). The findings of several studies and practitioner reports also substantiate the notion that well-equipped employees with a future-oriented mentality emerge as pivotal ISec assets whose potential is actualized to fortify organizational ISec (Hsu et al., 2015; Posey et al., 2013; Turel et al., 2020; Vance et al., 2015). For instance, security experts have emphasized that organizations should promote ISec through employees' personal accountability and proactive behavior in protecting digital privacy, implementing security best practices, and safeguarding against common cyber threats (NCSAM, 2019).

In our study, which reflects the shift in attention toward employee proactivity in managing cyber threats, we concentrate on employees' proactive information security behaviors (ISBs). ISBs are self-initiated, future-oriented behaviors characterized by a sense of situational control aimed at improving the information security situation within the workplace. Here, proactivity infers that employees anticipate potential future security complications or modifications, thereby facilitating appropriate preemptive action to improve existing security practices. Proactive employees are vigilant in identifying potential security risks and vulnerabilities within organizations and constantly seek ways to improve security practices. Proactive ISec encapsulates an array of processes and activities carried out within an organization with the objective of risk prevention. This involves, for instance, proactively helping organizations in the exploration of novel security protection technologies and methodologies, identifying much-needed work procedures to mitigate security risks, and engaging in the evaluation of the organizational security posture (Jaeger & Eckhardt, 2021; Shin & Lowry, 2020). This ongoing pursuit of improvement is essential in the dynamic landscape of information security, in which new risks and attack vectors continually emerge.

Previous studies have highlighted the strategic value of employee proactivity in mitigating evolving cybersecurity threats. However, our review of prior ISec research indicates that much of this work has focused on the factors influencing employee compliance with or violation of ISec policies. These studies

frequently employ protection motivation theory (PMT), deterrence theory, or related theories (Boss et al., 2015; Burns et al., 2023; Chen et al., 2021; Cheng et al., 2013; D'Arcy et al., 2009; Hovav & D'Arcy, 2012; Johnston et al., 2015; Lowry & Moody, 2015; Vance et al., 2020; Yazdanmehr et al., 2020). Although these theoretical adaptations offer invaluable insights, their origins in disciplines such as criminology, health, and ethics limit their ability to effectively explain and predict employees' proactive ISBs. For example, deterrence theory focuses on sanctions and outcomes allocated by the organization, in which employees are considered passive, reactive respondents to their context. As Parker et al. (2006) emphasized, employees' proactive behavior is qualitatively different from compliance behavior, thus precluding the assumption that the antecedents of both behaviors are identical. Given these considerations, we argue that a departure from the conventional ISec theoretical approach is essential for theorizing and empirically examining the drivers underlying employees' proactive ISBs. Accordingly, in our study, we advocate the application of proactive motivation theory (ProMT), which is unrelated to PMT, as our guiding theoretical framework for investigating the motivational factors that contribute to employees' proactive ISBs.

Grounded in ProMT, our study is the first to operationalize and empirically test proactive motivation in the context of information security in organizational settings. ProMT emphasizes the significance of proactive goal generation and its influence on employee behavior (Parker et al., 2010); thus, we leverage ProMT to delve deeper into the drivers of employees' proactive ISBs. Proactive goal generation entails envisioning and planning goals with the intention of shaping a different future by making changes to oneself or the environment. This process is driven by motivation and consciousness and is directed toward achieving specific objectives (Parker et al., 2010). For employees to be motivated to engage in proactive behaviors, ProMT asserts that they need confidence in their ability to initiate proactive goals and handle any potential consequences. This self-assurance empowers them to take proactive actions without fear of negative outcomes. Beyond self-confidence, employees require a compelling reason or perceived necessity to undertake proactive goals to serve as a driving force behind their proactive behavior. Affect-related motivational states also play a leading role in influencing proactive behavior. Emotions, such as enthusiasm, excitement, or a sense of fulfillment, can serve as catalysts for individuals to engage in proactive actions. Therefore, we propose the first research question:

RQ1. How and why are employees motivated to perform proactive ISBs at the workplace?

Both the ProMT and ISec research suggest that contextual variables and individual differences could influence employees' motivations to engage in desirable ISBs. ProMT studies highlight the critical role of contextual variables, such as leadership, work design, climate, and social processes, in fostering employees' proactive motivational states and proactive behaviors (Parker et al., 2010). Previous ISec studies have also investigated the effects of various contextual variables on employees' perceptions and ISBs (Hu et al., 2012; Posey et al., 2015; Shropshire et al., 2015), including transformative leadership, ethical climate,

organizational support, organizational structure, position, and time constraints. However, most of these contextual variables are broad and lack context specificity.

Individual differences have also been considered influential factors that interact with contextual variables to shape individuals' motivations and behaviors (Parker et al., 2010). However, we found that individual differences have received relatively less attention in the ISec literature. Only a limited number of previous ISec studies have investigated the role of Big Five personality traits and negative affectivity in influencing employees' perceptions and security behaviors (Johnston et al., 2016). Consequently, there is a need for a more comprehensive understanding of how individual differences influence the translation of perspectives induced by contextual variables into employees' ISBs (Johnston et al., 2016). Considering these opportunities, we propose the second research question:

RQ2. What and how do contextual variables and individual differences influence employees' motivations and proactive ISBs?

Accordingly, we expect to make several notable contributions to ISec research with our study. *First*, we propose a contextualized research model that identifies motivational factors that induce ISBs by employees from the perspective of proactivity. We operationalize proactive ISBs as self-initiated and future-oriented behaviors and advance the current understanding of motivational factors that influence employees' ISBs by empirically examining the influence of contextualized can-do, reason-to, and energized-to motivations (Parker et al., 2010) on proactive ISBs. We thus concur with other scholars that contextualization is foundational to strong theorizing in IS (Chen et al., 2021; Hong et al., 2014; Luo et al., 2020).

Second, we extend ProMT and prior ISec research to include supervisory ISec support as the context-specific antecedent of proactive motivational states. Specifically, we provide detailed insights into how supervisory ISec support influences employees' proactive motivational states and proactive ISBs. Incorporating the context-specific variable into ProMT would establish the theory's effectiveness when translated into an ISec context.

Third, we develop an integrated multilevel research model that identifies the interaction effects of proactive personality (as an individual-level variable) and supervisory ISec support (as a department-level variable) on employees' proactive ISBs, which has received little attention in previous research (Johnston et al., 2016). Thus, we extend both ProMT and ISec research by revealing how individual differences and contextual factors at different levels interact to influence employees' motivational states and behaviors. Our integrated framework thus contributes to a comprehensive understanding of the multilevel antecedents of proactive ISBs.

2 LITERATURE REVIEW

In this literature review, we first examine the prevalence of research on employees' ISBs concerning policy compliance and noncompliance, along with their respective antecedents. We then explain why these

antecedents may not be directly applicable to proactive behaviors. Next, we explore the contextual variables and individual differences that have been reported as relevant in studying employees' ISBs. Finally, we discuss how our proposed contextual factors and individual differences can contribute novel insights into the current understanding of employees' proactive ISBs.

2.1 Employees' ISBs

The ISec research literature broadly recognizes that employees' ISBs are closely tied to the effectiveness of organizational ISec policies (ISPs) (Hsu et al., 2015; Posey et al., 2013; Turel et al., 2020; Vance et al., 2015). A major body of research has focused on investigating the motivational factors driving compliance (and noncompliance) with ISPs, which emphasize adherence to formalized procedures, guidelines, roles, and responsibilities established by organizations to safeguard their information and technology resources (Cram et al., 2019; Lowry et al., 2017; Moody et al., 2018). Accordingly, the theoretical underpinnings of this research stream leverage theories developed in the fields of criminology, health, and ethics, thereby identifying a variety of antecedents of security policy compliance (Barlow et al., 2018; Bulgurcu et al., 2010; Chen et al., 2021; Chen et al., 2012; D'Arcy & Lowry, 2019; Siponen et al., 2014).

Again, we emphasize that *proactive behaviors*, in contrast to ISB compliance, represent employee behaviors that benefit organizations. Proactive behavior signifies that an "employee *anticipates*, *plans for*, *and attempts to create a future outcome* that has an impact on the self or environment" (Grant & Ashford, 2008a, p. 9; emphasis added). Despite their importance in contemporary security management (Hsu et al., 2015; Posey et al., 2013; Turel et al., 2020; Vance et al., 2015), the antecedents of proactive ISBs are inadequately understood. Given the distinct difference between compliance and proactive behaviors, the commonly reported antecedents in the ISec literature might not fully explain the motivational factors that drive self-initiated behaviors that lie beyond ISP or work-role requirements.

To illustrate, let us consider the factors identified in a meta-analysis conducted by Cram et al. (2019). They observed medium or large effect sizes for the influence of motivational factors such as personal norms, normative beliefs, perceived responsibility, response efficacy, and self-efficacy on employee compliance behavior. However, we argue that these motivational factors are insufficient to predict an employee's proactive ISBs for several reasons. For example, *personal norms* refer to an individual's personal moral beliefs about the appropriateness of a behavior (Harrington, 1996); such beliefs may explain employee ISP compliance. However, when it comes to motivating employees to engage in proactive ISBs, the mere belief in the appropriateness of a behavior falls short. ISP responsibility centers on the degree to which employees feel responsible for ensuring ISP compliance. To be motivated to take initiative, employees must assume personal responsibility for problems and goals beyond their mandated tasks (Parker et al., 2006). Likewise, in the ISec context, self-efficacy pertains to a person's confidence in their ability to perform recommended security actions (Johnston & Warkentin, 2010). Employees with high self-efficacy are more likely to

comply with policies or perform recommended security actions. Although individual creativity has been linked to proactive security behaviors in recent research (Lin et al., 2022), prior research has drawn on the theory of organizational citizenship behavior to explain the influence of creativity from the perspective of ability and competence in taking action to respond to threats. However, to engage in proactive ISBs, employees need to have pre-action confidence in their ability to pursue proactive goals and effectively manage the potential consequences of their actions.

Whereas previous research has revealed factors influencing employees' ISBs, our study aims to provide a deeper understanding of the distinct motivational factors that drive employees' proactive ISBs. Parker et al.'s (2010) ProMT provides a more comprehensive view of proactive behavior, positing that it is fundamentally driven by three proactive motivational states: can-do, reason-to, and energized-to motivations. These motivational states are influenced by various individual and contextual predictors. Our study is the first to use ProMT to examine employees' ISBs. Additionally, by examining contextual variables and individual differences, we aim to extend existing knowledge and offer new insights into the complexities of proactive ISB behavior. Before we introduce our own contextual and individual variables, the following subsection will review the contextual variables and individual factors that have been theorized and empirically tested in previous studies.

2.2 Individual-Difference and Contextual Factors Influencing Employees' ISBs

ISec research has also shown that contextual variables and individual differences are critical determinants that influence employees' ISBs. Within the organizational context, managerial support and organizational culture are recognized as salient factors. For example, previous studies have found that transformative leadership and paternalistic leadership positively influence employees' ISP compliance by increasing employees' organizational commitment (Guhr et al., 2019; Zhu et al., 2023). Several studies have underscored the influence of management support and involvement (Hu et al., 2012; Posey et al., 2015; Shropshire et al., 2015). For example, management participation was found to be positively related to employees' perceived control over compliance (Hu et al., 2012). Gwebu et al. (2020) revealed how ethical work climates distinctly influence employees' cognitive appraisals of ISP compliance costs and benefits. Chen et al. (2019) investigated the moderation effect of ethical climate on the relationship between moral disengagement and ISP violations. Hu et al. (2012) also reported the proactive role of organizational culture in influencing employees' ISP compliance by enhancing employees' positive attitudes, subjective norms, and behavioral control over compliance.

In contrast to contextual variables, little research has explored the influence of individual differences, such as Big Five personality traits (Johnston et al., 2016), low self-control (Burns et al., 2023), and negative affectivity (Posey et al., 2011) on employees' motivations and ISP compliance. For example, Johnston et al. (2016) reported that employees with a strong stability meta-trait exhibit a higher degree of risk aversion,

hence being less likely to violate ISP that places them at risk of threat- and sanction-related consequences. Posey et al. (2011) suggested that negative affectivity could lead to reduced trust when employees encounter heightened internal security measures within their organizations. Johnston et al. (2016) acknowledged the significance of individual characteristics in influencing employees' ISBs. They argued that it is critical to identify additional individual differences that could influence employees' ISBs and to enhance the current understanding of how individual differences influence the translation of perspectives derived from contextual variables into employees' ISBs.

Although prior ISec studies have examined the role of contextual variables and individual characteristics in influencing employee ISP compliance or noncompliance, the specific context-related variables that drive proactive employee's ISBs remain unidentified or empirically untested. Generalized leadership and climate variables, which lack context specificity, are weak predictors of specific outcomes (Hong et al., 2016). Previous ISec research has primarily investigated the effects of general management support, such as valuing employee contributions to the organization's welfare, or leadership traits, such as transformative leadership, on employee ISP compliance or noncompliance. These studies, along with the Parker et al. (2010) model, overlook the role of supervisor behaviors in shaping employee motivations and behaviors within their specific contexts. In particular, Parker et al. (2006) argued that general leader support or a leadership personality may play a negligible role in influencing proactive behavior, since leaders may not necessarily act in ways that stimulate proactivity. Echoing this point, we assert that it is essential to identify specific contextual variables that can trigger proactive motivational states and behaviors among employees.

Accordingly, our study identified supervisory support as a key contextual driver of employees' proactive motivational states and proactive ISBs. Supervisory support is evident when supervisors "show concern for employees' feelings and needs, encourage them to voice their own concerns, provide positive, chiefly informational feedback, and facilitate employee skill development" (Oldham & Cummings, 1996, p. 611). Individual differences in relation to proactivity indicate the tendency of an individual to be relatively unconstrained by situational forces in effecting environmental change. A proactive personality, characterized by a relatively stable tendency to initiate change in an environment (Bateman & Crant, 1993), is one of the most important traits for predicting proactive goals (Hong et al., 2016; Parker et al., 2006). However, proactive personality has not been investigated in the ISec literature. Thus, we focus on how proactive personality interacts with supervisory ISec support to influence employees' proactive motivational states.

3 THEORETICAL FOUNDATION

To better understand the process of employees' proactive ISBs and to identify those that may be the most useful in an ISec context, we leverage and carefully contextualize ProMT (Parker et al., 2010) as our

theoretical foundation for developing and testing a comprehensive multilevel model of the antecedents of proactive ISBs. Specifically, we leverage ProPMT to identify and empirically test the influences of proactive motivational states in the ISec context, while accounting for the impacts of individual differences and contextual factors on employees' proactive ISBs. We start by describing the goal-driven processes that yield the three motivational states addressed by ProMT. Parker et al. (2010) suggested that the three proactive motivational states are engendered by three processes that support proactive work behavior. That is, *can-do motivation* arises from employees' *confidence* in their ability to act proactively; *reason-to motivation* arises from the *internal forces* that drive employees' proactive behavior; and *energized-to motivation* arises from the *affect* that activates employees' propensity to engage in proactive behaviors. Prior research has demonstrated the important role of can-do, reason-to, and energized-to motivations in employees' proactive behaviors (Fuller et al., 2012). We examine these states in the context of encouraging employees' proactive ISBs by leveraging three associated constructs: role-breadth self-efficacy, flexible security role orientation, and proactive personality. On this foundation, we then operationalize additional contextualized hypotheses that can be used to test our theorization in the form of a research model. **Table 1** summarizes the three proactive motivational states, as well as this paper's resulting contextualized constructs.

Table 1. ProMT-Based Constructs Contextualized to ISec

ProMT Concepts	Explanation and Citations	Study Construct	Definition of Construct Used in Our Study
Can-do motivation	Perception of one's capacity to behave proactively (Parker, 1998; Parker et al., 2006)	Security role-breadth self-efficacy	Employees' perception of their capacity to carry out a range of behaviors that extend beyond their prescribed organizational ISec roles
Reason-to motivation	Internal means to enact proactive behaviors (Parker et al., 1997; Parker et al., 2006)	Flexible security role orientation	Employees' feelings of ownership of organizational ISec problems and goals beyond their immediate set of ISec tasks or formal responsibilities, thus seeing them as "my job" rather than "not my job" (Wall & Jackson, 1997)
Energized-to motivation	Emotional state that leads to proactive behavior (Seo et al., 2004; Warr, 1990)	Positive affect	Employees' fundamental feelings of pleasure and activation regarding ISec protection for their organization—including feeling enthusiastic, excited, inspired, and joyful
Individual differences	Personal differences in relatively stable behavioral tendencies (Bateman & Crant, 1993; Parker et al., 2006)	Proactive personality	"A dispositional measure of individual proactivity that will persist across contexts and over time" (Hong et al., 2016, p. 692)
Contextual factors	"Situational or environmental stimuli that impinge upon focal actors and are often located at a different level of analysis from those actors" (Johns, 2018, p. 22).	Supervisory ISec support	A supervisor's concern for employees' ISec-related feelings and needs, conveyed by encouraging them to voice their own ISec concerns and providing positive and chiefly informational feedback regarding ISec issues (Deci & Ryan, 1987)

Consistent with ProMT, to address **RQ1**, our research model hypothesizes that three proactive motivational states influence employees' proactive ISBs. First, we predict that employees with high levels of security RBSE will be more confident in taking proactive steps to protect their organization. Second, employees with highly flexible security roles will feel increased personal responsibility to proactively protect organizational ISec. Third, employees with positive affect will treat security threats more positively (than employees with negative affect) and do their best to resolve security issues. To address **RQ2**, we identify proactive personality as the key individual-difference construct and supervisory ISec support as the key contextual factor in our context. We propose that both enhance employees' proactive motivational states. **Figure 1** depicts our operationalized, testable model. In the next section, we further explain the underlying theory and contextualization that support the model's pathways.

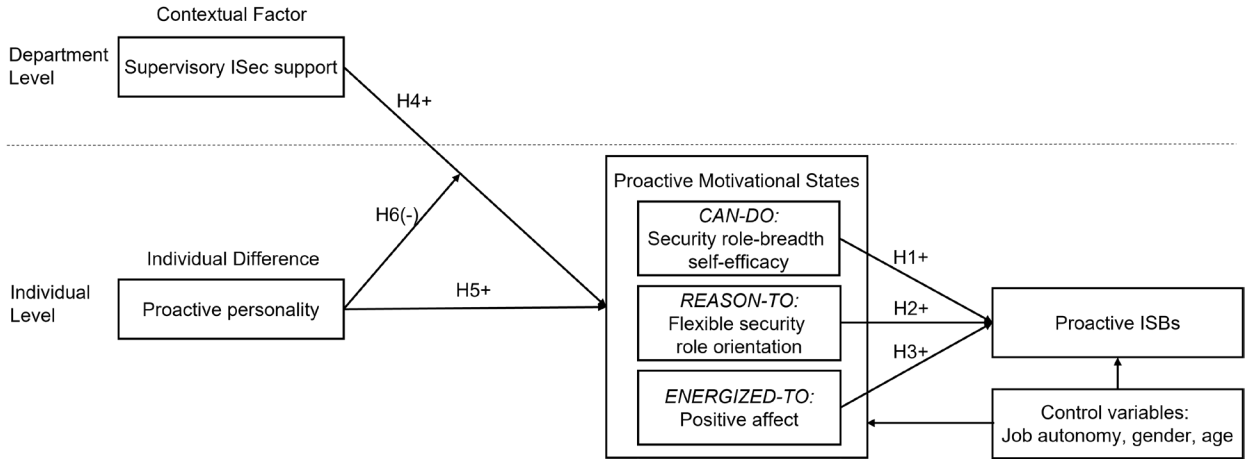


Figure 1. Theoretical Model of the Antecedents of Proactive ISBs

4 HYPOTHESIS DEVELOPMENT

4.1 Can-Do Motivation and Role-Breadth Self-Efficacy (RBSE)

The first goal-driven process, which produces the can-do motivational state, is related to confidence. It is fostered when people engage in proactive behaviors because they believe they are in control of their own actions and can manage the potential consequences. Scholars have employed theories that address expectancy, control, and self-regulation (Morrison & Phelps, 1999; Parker et al., 2006) to argue that such beliefs play a key role in overcoming the psychological risks to which people subject themselves when they behave proactively. Can-do motivation answers the question, "Can I do this?" Employees must have the confidence to engage in proactive behaviors that open them to risks. For example, when an employee takes the initiative to improve work methods or procedures, others may resist this action or view it with skepticism (e.g., they may believe the employee is generating unnecessary work, trying to "look good," or attempting to get others in trouble. Similarly, proactive behavior involves risks, especially when it could lead to changes in an organization's status quo, and an employee who engages in such behaviors could thus be labeled a complainer or characterized as "difficult." Can-do motivation helps employees gain the

confidence to overcome the risks of and social resistance to engaging in these activities and thus fosters proactive behaviors (Parker & Wall, 1998).

To perform proactive ISBs that improve (or challenge) an organization's security status quo, employees need to have the confidence to set ambitious goals and overcome organizational barriers. Among the constructs related to can-do proactive motivation, the literature has devoted the most attention to *role-breadth self-efficacy* (RBSE), which is "the extent to which people feel confident that they are able to carry out a broader and more proactive role, beyond traditional prescribed technical requirements" (Parker, 1998, p. 835). RBSE is a form of self-efficacy, but it has important conceptual differences from the self-efficacy constructs typically examined in the ISec literature. First, in security research, self-efficacy is defined as "the degree to which an individual believes in his or her ability to enact the recommended response" (Johnston & Warkentin, 2010, p. 551). Moreover, self-efficacy involves an employee's ability to perform a specific behavior, whereas RBSE encompasses proactive behaviors that extend beyond an employee's prescribed tasks (Parker, 1998). Finally, previous research has found a positive relationship between RBSE and proactive behaviors (Ouyang et al., 2019; Parker et al., 2006). We thus propose *security RBSE*—that is, an employee's confidence in performing security activities that lie beyond their prescribed roles—as a pivotal factor that directly fosters or represents can-do proactive motivation.

Because proactive motivational states increase an employee's perceptions of control and of the likelihood of success (Parker, 1998), RBSE is positively related to proactive behaviors (Chen et al., 2013), creativity, and idea implementation (Parker et al., 2006). Today's organizations have undergone a dramatic shift that has made it necessary to account for ISec in all business processes (Jaeger & Eckhardt, 2021; Shin & Lowry, 2020) and to view security as a primary organizational governance concern (AlGhamdi et al., 2020); thus, ISec is no longer viewed as solely the responsibility of the IT department (Flores et al., 2014; Johnston & Hale, 2009). A recent study tied creativity to proactive ISBs (Lin et al., 2022). We thus propose that employees with high security RBSE are likely to have high levels of confidence in dealing with organizational ISec issues and are more likely to perform security-related actions proactively rather than merely complying with ISec rules or policies.

H1. An employee's security role-breadth self-efficacy is positively associated with the employee's engagement in proactive ISBs.

4.2 Reason-to Motivation and Flexible Role Orientation

It is crucial for employees to believe that a compelling reason exists to engage in proactive ISBs. One powerful reason is an employee's intrinsic motivation in the work activity, which can increase feelings of responsibility or ownership of goals and problems beyond their immediate set of tasks (Parker et al., 1997). The second goal-driven process, which yields the reason-to motivational state, is related to internal motivation and occurs when people engage in proactive work behaviors that are likely to fulfill their responsibilities, goals, or aspirations (e.g., achieving high levels of success in their careers). Reason-to

motivation maps onto theories that answer the question, "Why should I act?" For example, according to goal-setting theory (Locke & Latham, 1990) and self-determination theory (Deci & Ryan, 2000), in addition to needing to feel in control, people are motivated to engage in proactive behavior when they have a strong internal motivation, such as defining their role broadly or feeling responsible for longer-term organizational goals. Because proactive behavior is self-initiated, employees internalize the proactive behaviors they perform and perceive them as their own. Thus, compared to externally motivated employees, employees motivated by a personal sense of responsibility to behave proactively are more likely to view such expanded workplace roles as "my job" rather than "someone else's job."

Extant ISec research has concluded that personal responsibility plays a role in influencing employees' ISP compliance behavior (Yazdanmehr & Wang, 2016). Whereas personal responsibility concerns the degree of an employee's perceived responsibility to comply with ISPs, employees with a *flexible security role orientation* feel more responsible for overcoming organizational problems even if the responsibilities extend beyond their prescribed tasks (Parker et al., 2006). Flexible role orientation has been seen as an indicator of employees' internalization of external values and regulatory structures (Parker & Ohly, 2008). Research has explained the positive effect of flexible role orientation on proactive work behavior (Parker et al., 2006) and has described flexible role orientation as employees' feelings of ownership of security goals and problems that lie beyond their required security tasks. We thus propose that flexible security role orientation directly fosters reason-to motivation, which enables employees' proactive ISBs.

When facing security threats, employees with a highly flexible security role orientation exhibit an increased likelihood of taking action to resolve security issues that lie beyond their job requirements. Employees with reason-to motivation are likely to maintain a high level of interest and enthusiasm (Gagné & Deci, 2005; Hong et al., 2016), pursue proactive goals, and overcome the difficulties that may arise in the process of doing so (Parker et al., 2010). Thus, employees with a flexible security role orientation feel a strong personal responsibility to support the organization's security goals and to overcome risks in the process of performing proactive ISBs because proactivity gives such employees a sense of accomplishment (Gagné & Deci, 2005). We consequently propose that employees who have a flexible role orientation in terms of protecting organizational ISec have increased engagement in proactive ISBs.

H2. An employee's flexible security role orientation is positively associated with the employee's engagement in proactive ISBs.

4.3 Energized-to Motivation and Positive Affect

In addition to can-do and reason-to motivations, employees need sufficient positive affect to engage in proactive ISBs. The third goal-driven process, which yields the energized-to motivational state, relates to affect and occurs when people have enough positive affect to feel sufficiently energized to engage in proactive behaviors. Core affect reflects people's feelings, including both valence (e.g., positive or negative) and activation (Russell, 2003). Research has theorized that positive affect can broaden momentary

thought-action repertoires and is likely to activate approach tendencies whereby people anticipate positive future outcomes and use active strategies to achieve goals (Seo et al., 2004). Research has also theorized that positive affect can broaden thinking when dealing with problems (Fredrickson, 1998). Moreover, positive affect encourages people to set more challenging goals (Ilies & Judge, 2005) and to engage in activities that might have negative consequences (Oettingen et al., 2005). Positive affect is therefore a strong predictor of employees' goal-setting and engagement in proactive behaviors.

Because proactive behavior is inherently emotional, employees who engage in it may put their organizational status at risk (Grant & Ashford, 2008b). Positive affect reflects people's feelings and can activate their approach action tendencies (Fredrickson, 1998). Likewise, employees with a high level of positive affect are more likely to assess their current actions favorably (Hong et al., 2016; Seo et al., 2004). Previous research has suggested that highly activated positive affect, such as feeling inspired, exerts a stronger positive influence on employees' proactive behavior than does inactivated affect. Furthermore, prior research has revealed that highly activated positive affect has a positive influence on employees' proactive behaviors (Hong et al., 2016); thus, we investigate *positive affect* as the primary representation of and immediate cause of energized-to motivation.

Research has consistently demonstrated a positive relationship between positive affect and proactive behaviors, such as taking personal initiative (Hong et al., 2016). In the ISec context, positive affect has been found to positively influence employees' attitudes toward ISP compliance (Burns et al., 2019; D'Arcy & Lowry, 2019); however, the influence of positive affect on proactive ISBs has not been investigated. Positive affect can broaden people's thinking and thereby motivate them to address problems using a variety of approaches (Seo et al., 2004). Thus, we expect that employees with high levels of positive affect will demonstrate broadened thinking when addressing security problems. Positive affect may motivate employees to perform proactive ISBs because people with high levels of positive affect are prone to focus more on the positive outcomes of their actions and will assess these outcomes in a more favorable way than those with negative affect (Parker et al., 2010). Such individuals' favorable judgment and positive interpretation of proactive ISBs may lead to high levels of engagement in proactive ISBs. We thus hypothesize the following:

> **H3.** An employee's positive affect is positively associated with the employee's engagement in proactive ISBs.

4.4 The Key Contextual Factor of Proactive Motivation: Supervisory Support

Finally, we propose that the contextual factor of supervisory ISec support can influence the three proactive motivational states and thus foster or discourage employees' proactive ISBs. *Context* is defined as "situational or environmental stimuli that impinge upon focal actors and are often located at a different level of analysis from those actors" (Johns, 2018, p. 22). Research has suggested that supervisors who

encourage desired behaviors may promote proactive motivational states (Madjar et al., 2002). Likewise, ProMT research has emphasized that it is crucial to identify what kinds of supervisory support promote proactive motivational states among employees (Parker et al., 2006). Research has also found that encouragement by leaders influences employees' RBSE and autonomous motivation and may motivate them to engage in proactive behaviors (Wu & Parker, 2017). That is, employees will have the confidence and motivation to enact changes in their work environment if they receive support from their supervisors (Chen et al., 2016; Oldham & Cummings, 1996). Because *supervisory support* involves a focus on employees' feelings and needs, on encouraging them to have a voice, and on the provision of positive feedback, it is likely to facilitate employee proactivity (Oldham & Cummings, 1996). We extend the related research on supervisory support (Tucker et al., 2008; Wu & Parker, 2017) by proposing that supervisors who express concern for employees' security-related feelings and needs, encourage employees to voice their own security concerns, and provide positive informational feedback can strengthen employees' three proactive motivational states and thereby motivate them to engage in proactive ISBs.

First, can-do motivation concerns employees' confidence in performing proactive behaviors. Highly supportive supervisors encourage employees to achieve personal goals and support their decisions and actions. Encouragement, as a type of persuasion, endows the recipient with an increased sense of competence (Bandura, 1999). Previous ISec research has investigated the positive role of manager support in improving employees' self-efficacy in performing recommended security actions (Hu et al., 2012). We conceptualize can-do motivational states in terms of RBSE, which emphasizes employees' confidence in performing security actions that lie beyond their prescribed tasks. Previous research has suggested that to deal with potential obstacles to and consequences of proactivity, employees should be able to receive help and support from supervisors (Parker et al., 2006). Therefore, we argue that a work environment with high-level supervisory ISec support encourages employees to take the initiative to protect the organization's security and thus to feel increased confidence in resolving security issues. This confidence reflects a high level of security RBSE, and our theoretical rationale thus aligns with previous findings on the relationship between leader support and RBSE (Wu & Parker, 2017).

Second, reason-to motivation provides employees with reasons to be proactive. Employees with a highly flexible role orientation will feel more responsibility and ownership concerning problems that lie beyond their prescribed roles (Parker et al., 2006). Supervisory support that encourages employees to pursue their own ideas creates a positive environment in which employees can choose goals according to their interests (Sheldon & Elliot, 1999). Previous studies have surmised that a good security culture may increase employees' perceived norms or responsibility for protecting organizational security (Yazdanmehr & Wang, 2016). Likewise, in an environment in which employees perceive strong supervisory ISec support, they are more likely to take responsibility for resolving security issues than with weak support. Employees are more

likely to have a highly flexible security role orientation when encouragement from supervisors fosters an increase in self-determination (Oldham & Cummings, 1996) and encourages employees to engage in self-concordant goal setting (Parker et al., 2006). Thus, we propose that employees are more likely to feel ownership of security goals and problems that lie beyond their immediate set of security tasks and to thereby exhibit a highly flexible security role orientation (Parker et al., 1997) in an environment characterized by strong supervisory ISec support.

Third, energized-to motivation relates to a person's emotional impetus to behave proactively. High levels of positive affect give rise to the positive energy necessary to stimulate employees' proactive behavior (Parker et al., 2010). Leadership behaviors are crucial affective events that influence employees' positive (or negative) affective states (Dasborough, 2006), and we explain how supervisory ISec support influences security-related positive affect among employees: First, supportive supervisors care about the needs of employees (Oldham & Cummings, 1996) and reinforce employees' autonomy in decision-making and work engagement (Niessen et al., 2017). By providing thoughtful ISec support, supervisors demonstrate that they care about the security of the data assets of employees and the organization. Employees who perceive that the organization cares about their well-being experience positive affective states (Caesens et al., 2016; Luu, 2018). Employees with supportive supervisors are also more likely to perceive proactive ISBs as valued and respected by their supervisors and are more likely to perceive increased opportunities to improve their organizational position and performance than those without supportive supervisors (Wang et al., 2019). In turn, employees prone to achieving higher levels of performance tend to experience higher positive affect than those with lower performance (Baron, 1990). We thus posit that supervisory ISec support is related to higher levels of positive affect.

> **H4**. An employee's perception of supervisory ISec support is positively associated with the employee's proactive motivational states, that is, (a) security role-breadth self-efficacy, (b) flexible security role orientation, and (c) positive affect.

4.5 The Key Individual Difference in Proactive Motivation: Proactive Personality

Among the several kinds of individual differences (e.g., personality, life values, knowledge, and skills) that Parker et al. (2010) identified as exerting the strongest influence on the three proactive motivational states, the most frequently investigated is *proactive personality*, which is the "behavioral tendency to identify opportunities, show initiative, take action, and to persevere to bring about change" (Parker et al., 2006, p. 640). The role of proactive personality in stimulating proactive behavior among employees has been extensively investigated (Crant, 1995; Hong et al., 2016; Parker et al., 2006). Research has suggested that employees with a highly proactive personality have an increased likelihood of identifying opportunities to initiate change (Parker et al., 2006). Crucially, research has shown that a proactive personality positively influences an employee's proactive motivational states, including can-do (Brown et al., 2006), reason-to

(Parker et al., 2006), and energized-to (Li et al., 2020; Li et al., 2017) states. Our study thus identifies proactive personality as the individual difference that exerts the strongest influence on employees' proactive motivational states, which we address next.

First, a proactive personality can increase an employee's RBSE (Parker & Wall, 1998; Parker et al., 2006) or job-search self-efficacy (Brown et al., 2006). We propose that a highly proactive personality also increases an employee's security RBSE. Proactive people are considered self-initiated, change oriented, and future focused (Parker & Collins, 2010). These positive characteristics enable people to be less constrained by external factors and more likely to find and implement their own improvement solutions than less-proactive people (Bateman & Crant, 1993). Thus, proactive people are likely to be confident in performing security activities beyond their prescribed work role (Parker et al., 2006). We thus posit that employees with a highly proactive personality are more confident in identifying and acting on opportunities to solve security problems. Conversely, less-proactive employees are less likely to feel capable of acting proactively but may still follow organizational policies when facing security threats, assuming they have sufficient self-efficacy and are not experiencing undue job stress or role overload (Chen et al., 2018).

Second, Parker and Sprigg (1999) and Parker et al. (2006) demonstrated a positive relationship between proactive personality and flexible role orientation. Proactive people are characterized as self-created (Bateman & Crant, 1993) and feel responsible for improving situations (Kim et al., 2009). Thus, compared to less-proactive employees, when proactive employees experience security issues in their daily work, they are more likely to incorporate additional security activities into their roles. Consequently, to actively address security issues, proactive employees are likely to define their roles more broadly (Parker et al., 1997) or redefine their roles (Frese & Fay, 2001). We thus propose that employees with a highly proactive personality are more likely to feel responsible for taking proactive steps to protect organizational security and more likely to have a highly flexible security role orientation.

Third, employees with a highly proactive personality tend to experience increased positive affect while at work (Li et al., 2020; Li et al., 2017) and decreased negative emotions, such as emotional exhaustion or burnout (Alarcon et al., 2009; Jawahar et al., 2012). Employees with a highly proactive personality are likely to experience increased positive affect in protecting organizational security because proactive people tend to actively strive to attain goals, solve problems, and maintain strong control over their emotions (Bateman & Crant, 1993). Previous research has found that employees with a highly proactive personality are more likely to positively reinterpret a situation to reduce negative emotions (Park & DeFrank, 2018). Thus, proactive employees are likely to reinterpret a security situation positively to reduce negative emotions. In the ISec context, employees with a highly proactive personality are likely to be less influenced by the negative outcomes of their actions than less-proactive employees and more likely to experience positive affect. We thus hypothesize:

H5. The degree to which an employee has a proactive personality is positively associated with the employee's proactive motivational states, that is, (a) security role-breadth self-efficacy, (b) flexible security role orientation, and (c) positive affect.

4.6 Interaction Between Supervisory ISec Support and Proactive Personality

Parker et al. (2010) indicated that contextual variables may interact with individual differences to influence employees' proactive motivational states. For example, one study demonstrated that individual differences, such as subordinates' need for independence, affect the influence exerted by leaders (Kerr & Jermier, 1978). Due to the key attributes related to proactive motivational states (Parker et al., 2010), employees with a highly proactive personality are likely to have strong can-do, reason-to, and energized-to motivations. Thus, we argue that proactive personality influences the effect of supervisory ISec support on employees' proactive motivational states for three reasons.

First, employees with a highly proactive personality are predisposed to experience strong motivational states and take initiative in their personal environments (Lee et al., 2014; Thompson, 2005); for example, they act on their plans irrespective of situational forces or take initiative based on their own ideas. Thus, proactive employees are likely to be more confident in dealing with security issues in the workplace, regardless of supervisory support. Proactive employees are more likely to have high levels of RBSE than less-proactive employees (Parker et al., 2006). Such employees do not need to receive supportive cues from supervisors to perceive the RBSE needed to perform proactive ISBs. Thus, we argue that the effect of supervisory ISec support on employees' security RBSE is weakened by proactive personality.

Second, because highly proactive employees are predisposed to proactively engage in ISBs rather than waiting to be instructed to do so by their supervisors (Fuller & Marler, 2009), they are likely to have higher levels of intrinsic autonomy (Gagné & Deci, 2005) than less proactive employees. Thus, employees with a highly proactive personality require less support from supervisors to adopt a flexible security role orientation. On the basis of self-motivation, proactive employees are able to engage in self-leadership to successfully perform a range of proactive behaviors that lie beyond their prescribed tasks (Rosenbach, 2018); the flexibility of their security role orientation is hence less affected by supervisors' behavior.

Third, less proactive employees tend to use whatever internal resources they have, including support from supervisors, as motivation to accomplish a task and overcome the negative consequences of doing so (Hobfoll et al., 1990). For example, as (Lloyd et al., 2015) argued, supervisory support may reduce employees' emotional exhaustion. However, proactive employees have an inherent tendency to positively reinterpret security situations to overcome negative attitudinal and emotional perceptions. Because such employees do not rely strongly on cues from their supervisors to overcome negative emotional perceptions, the effects of supervisory ISec support on their positive affect are relatively weak. Thus, we propose the following hypothesis:

H6. An employee's perception of supervisory ISec support negatively interacts with proactive personality such that the higher the degree to which an employee has a proactive personality, the lower the degree to which supervisory ISec support will be positively associated with the employee's proactive motivational states, that is, (a) security role-breadth self-efficacy, (b) flexible security role orientation, and (c) positive affect.

5 RESEARCH METHODOLOGY

We administered a cross-sectional survey across 55 departments in a variety of organizations to explore the antecedents of employees' proactive ISBs. Formally, we adopted a multilevel perspective and used multilevel modeling to investigate the effects on departments and employees in those departments.

5.1 Sampling and Procedures

We used a snowball sampling procedure to survey employees from various work departments across organizations in the electronics, banking and finance, education, IT services, and manufacturing sectors. All the participants were Chinese employees recruited from Mainland China and Taiwan who responded to the survey in Chinese. First, we identified an appropriate full-time employee in each organization to serve as our contact person. Most of the contact persons were alumni of the universities where the authors worked. Second, each contact person was asked to complete a questionnaire. Each contact person then passed on a unique survey link to colleagues who had the same supervisor and asked them to participate in the survey. The participants were asked to complete a survey containing measures of proactive motivational states, perceptions of supervisory ISec support, proactive personality, proactive ISBs, and demographic information. Each respondent was paid ¥25 or NT$100 (approximately US$4) for their participation, and all the respondents were assured that their answers would remain confidential and that organizational representatives, including their supervisors, could not access their responses.

The questionnaire was translated into Chinese following the procedures outlined by Brislin (1980), and the translation was carried out by ISec researchers proficient in Chinese and English. Two researchers developed a Chinese version of the survey, and another researcher back-translated the survey into English to ensure that the interpretation of survey items contained no discrepancies. We received a total of 232 responses. Following Guzman and Espejo (2019), for a department to be included in our study, we required responses from at least two employees from the same department. After we eliminated work departments from which only one employee responded to our questionnaire and removed respondents who did not pass the attention check, our final sample consisted of 210 employees from 55 departments.

As a general rule, increasing the sample size can improve estimation accuracy in terms of fixed and random effects on all levels (Maas & Hox, 2004). Our sample size at the department level was 55; fortunately, this was higher than the high-level sample size of 50 recommended for multilevel data analysis (Maas & Hox, 2005). Of the 210 respondents, 50.5% were male, and 51.4% were between the ages of 30 and 39. In addition, more than 60% of the respondents had an undergraduate degree. Respondent

characteristics in terms of gender, age, tenure, education, and industry type are summarized in **Table 2**.

Table 2. Demographic Information

Measure	Category	No.	%	Measure	Category	No.	%
Age	Between 18 and 29	62	29.5	Gender	Male	106	50.5
	Between 30 and 39	108	51.4		Female	104	49.5
	Between 40 and 49	35	16.7	Industry	Banking and finance	67	31.9
	Between 50 and 59	5	2.4		IT services	67	31.9
	60 or older	0	0		Electronics	18	8.6
Tenure (years)	⩽ 3	88	41.9		Manufacturing	15	7.1
	> 3 to 6	38	18.1		Construction	6	2.9
	> 6 to 10	49	23.3		Education	6	2.9
	> 10	35	16.7		Retail, wholesale	5	2.4
Education	High school	0	0		Professional services	5	2.4
	Some college	8	3.8		Communications	3	1.4
	Undergraduate degree	130	61.9		Insurance	3	1.4
	Master's degree	70	33.3		Audit	2	1.0
	Doctoral degree	2	1.0		Other	11	5.2

5.2 Measurement Variables

All the measurement variables were based on highly validated measures and distinct anchors from the extant literature, which are fully detailed in **Appendix A**. An expert review panel was conducted to increase the content validity, face validity, and realism of all items. The expert review panel was knowledgeable about security research and instrument design; based on their feedback, the items were adapted to the ISec context. Here, we introduce these items in terms of the dependent variable, individual-level variables, department-level variables, and control variables.

5.2.1 Dependent Variable: Proactive ISBs

The measurements of proactive ISBs were adapted to the ISec context from Morrison and Phelps (1999) and Hofmann et al. (2003). Proactive ISBs center on employees' self-initiated, changed-oriented, and future-oriented behaviors intended to improve organizational ISec. We conducted a small field study to identify the most proactive and realistic ISBs for the ISec context. We did so by first providing definitions and examples of proactive ISBs to 14 Chinese employees from various Chinese organizations who had ISec experience. Each employee was asked to code the proactive ISB items on a five-point scale from 1 (not proactive at all) to 5 (very proactive). The employees also indicated the extent to which these behaviors were realistic in their work context on a scale from 1 (not realistic at all) to 5 (very realistic). The behaviors that earned a rating of 4 or 5 were considered proactive ISBs. Based on the average rating, we chose five items for which the ratings for both proactivity and realism were above 4.

5.2.2 Individual-Level Variables Used as Predictors

Our individual-level measurement focused on proactive motivational states, positive affect, and proactive personality. To better measure the *proactive motivational states* construct, the measurements of security RBSE and flexible security role orientation were adapted to the ISec context from Parker et al. (2006). To

measure positive affect, we used four items from Warr (1990): enthusiastic, excited, inspired, and joyful. The measurement of proactive personality was adopted from Claes et al. (2005).

5.2.3 Department-Level Variables

Our department-level measurement focused on *supervisory ISec support*, for which we used a six-item measure adapted from Tucker et al. (2008) and Wu and Parker (2017) to assess each employee's perception of supervisory ISec support. Recall that to ensure that this was a proper department-level measure, we needed to receive evaluations of the same supervisor by at least two employees from the same department. We consequently aggregated employees' ratings of supervisory ISec support to create a department-level variable. We calculated the rWG(j) to estimate the extent of interrater within-group agreement. The results showed that the average rWG(j) value was higher than 0.70, indicating that the department average of supervisory ISec support could be used as an indicator of a department-level variable (LeBreton & Senter, 2008). In addition, the intraclass correlation coefficients ICC(1) and ICC(2) were calculated.[1] The value of ICC(1) was 0.371, $F_{(54, 155)} = 3.363$, $p < .001$. The results indicated that 37.1% of the variance in supervisory ISec support was explained by department membership, which is considered a large effect (LeBreton & Senter, 2008). The value of ICC(2) was 0.70, which suggested a high reliability of the mean of the department-level variable (Bliese, 2002).

5.3 Control Variables

To further address endogeneity and counter-explanations for our model, we also controlled for age, gender, and job autonomy. Age and gender have been found to be associated with employees' proactive behavior (Bolino & Turnley, 2005; Thomas et al., 2010), and research has identified job autonomy as a key contextual variable that influences employees' proactivity (Den Hartog & Belschak, 2012; Parker et al., 2006). The measurement of job autonomy was adopted from Morgeson and Humphrey (2006).

5.4 Reliability and Validity

We used AMOS 28.0 to analyze the measurement model. We conducted a confirmatory factor analysis (CFA) to examine the distinctiveness among the constructs of supervisory ISec support, job autonomy, proactive ISBs, security RBSE, positive affect, and flexible security role orientation. Overall, the resulting fit indices suggested that the hypothesized six-factor model fit the data well and that the indices were above suitable levels (Gefen et al., 2011) ($\chi^2_{(384)} = 696.706$, RMSEA = .06, CFI = .94, SRMR = .05).

Regarding the tests of reliability and validity, we assessed the reliability of all the constructs using composite reliability (CR) scores, and we assessed convergent validity using the average variance extracted (AVE) of each latent construct (Barclay et al., 1995). Discriminant validity was assessed by comparing the

[1] ICC(1) represents the proportion of total variance that can be explained by the department-level variable; ICC(2) indicates the reliability of the aggregate measure of the department-level construct.

square root of the AVE to the correlations among the other constructs (Fornell & Larcker, 1981). As **Table A.1** shows, the CR scores were greater than 0.9 and thus higher than the recommended level of 0.7, indicating acceptable reliability (Bagozzi & Yi, 1988). The AVE values were greater than 0.5 and thus indicated good convergent validity (Fornell & Larcker, 1981). Furthermore, the correlations among the constructs were less than the square root of the AVE (see **Table 3**), indicating good discriminant validity (Compeau et al., 1999). Finally, multicollinearity among the variables was assessed using the variance inflation factor (VIF). The results showed that the VIF values for the variables were acceptable, ranging from 1.2 to 1.8 (Petter et al., 2007). Thus, collinearity was not a serious issue.

Table 3. Measurement Model Statistics

Latent Constructs	Mean	SD	1	2	3	4	5	6	7
(1) Supervisory ISec support	5.57	0.74	**0.909**						
(2) Job autonomy	3.81	0.80	0.434	**0.828**					
(3) Proactive ISBs	4.00	0.48	0.500	0.215	**0.817**				
(4) Security role-breadth self-efficacy	3.50	0.73	0.443	0.354	0.538	**0.809**			
(5) Positive affect	3.44	0.77	0.394	0.248	0.522	0.539	**0.885**		
(6) Flexible security role orientation	3.92	0.62	0.516	0.268	0.626	0.603	0.573	**0.790**	
(7) Proactive personality	3.59	0.60	0.325	0.275	0.449	0.476	0.466	0.459	**0.728**

Note. Bolded and underlined numbers on the diagonal represent the square root of the AVE; ISec = information security; ISBs = information security behaviors; SD = standard deviation.

5.5 Testing Measurement-Model Invariance Across Groups

Because we surveyed two different groups (one from Mainland China and the other from Taiwan) but used the same measures for each group, we performed a measurement-model invariance test to determine whether the factor structure of the measurement model differed across groups. We performed configural invariance and metric invariance tests using AMOS 28.0.

For the configural invariance test, we tested the unconstrained model across groups. The results of the model fit statistics showed that the existing factor structure was a good fit for each group (χ^2/df = 1.85, RMSEA = .06, CFI = .90, SRMR = .05). For the metric invariance test, we assessed whether the indicators measured the same thing across groups. The results of the measurement-weights comparison showed that the chi-square difference was significant; thus, the model did not achieve full invariance. We then freed the constraints on each factor to identify the indicators that had the greatest influence on the chi-square statistic. After freeing the constraints of the three indicators, we received a nonsignificant invariance-test result (p = .083). According to the guidelines of Hair et al. (2010), our measurement model thus achieved partial metric invariance.

5.6 Common Method Variance and Nonresponse Bias

To reduce common method variance (CMV) and improve data quality, we followed the recommendations of Podsakoff et al. (2003). First, we conducted an expert review to increase content validity and decrease item ambiguity. Second, we used more than one scale format and employed different anchor points—such as disagree–agree and unlikely–likely—throughout the questionnaire. Third, the participants were assured

that the questionnaire was anonymous and that their information would not be shared. The questionnaire's introduction informed the participants that there were no right or wrong answers and encouraged them to answer honestly. Fourth, we divided the survey into two parts. The first part included the measures of supervisory ISec support and proactive motivational states. The second part included the measures of proactive ISBs, measures of proactive personality, and demographic information. After completing the first part, the participants were instructed to watch a short video for at least 30 seconds and answer a question related to the video. We chose a video unrelated to ISec to help clear the respondents' short-term memory. This separation of constructs is one of the most effective ways to avoid CMV (Podsakoff et al., 2003).

Two distinct analyses were performed to test for the effect of CMV. First, following Lindell and Whitney (2001), a marker variable technique was used. Adapted from Balozian et al. (2019), the items of the marker variable were "Please rate how swiftly your IT department is able to detect advances in technology that are relevant to the business" and "Please rate how quickly your IT department is able to detect changes in customer demand." The results showed that the correlations among all the latent variables and the marker variable were less than 0.3, which indicated that serious CMV was not present (Tehseen et al., 2017). We selected the second-smallest correlation of the marker variable and any other construct (r = 0.13) as the CMV estimate. The correlations among the theoretical constructs changed in magnitude but remained unchanged in significance.

Second, we used the unmeasured latent common method construct approach to detect CMV, in accordance with Podsakoff et al. (2003). The variance of the marker variable was set to 1, and the regression weights for all the relationships of the main constructs to the marker variable were constrained to be equal. Next, we conducted a CFA with and without this latent method factor. The results showed that the difference in variance between the two models was less than 3.84 in one degree of freedom, which indicated that CMV was not significant. Overall, the results of the two tests suggested that CMV was not of great concern.

An analysis of nonresponse bias was conducted by comparing employees' proactive ISB intentions among all the responses, the responses returned in the first week, and the responses returned in the final week. The *t*-test results of these timed waves showed no differences among any of the comparisons at an alpha level of 0.05 (Armstrong & Overton, 1977). Thus, nonresponse bias was likely not a serious issue.

6 ANALYSIS AND RESULTS

We used the mixed model function in SPSS 26.0 to test the integrated multilevel research model. This approach was appropriate because the multilevel results can be derived from a single model by incorporating random effects (Quené & Van den Bergh, 2004). Compared with the traditional generalized linear model, the SPSS mixed method allows for violations of sphericity in error structure, which are highly common in repeated measures data and can influence the interpretation of the results (Brouthers et al., 2014;

Quené & Van den Bergh, 2004). Several studies have used the SPSS mixed method similarly for multilevel data analysis (Coelho & Romão, 2018; Dumas & Perry-Smith, 2018; Quinones & Griffiths, 2017). Specifically, we estimated the effects of the department-level variable (i.e., supervisory ISec support) and the individual-level variable (i.e., proactive personality) on employees' proactive motivational states and proactive ISBs. As recommended by LeBreton and Senter (2008), the value of ICC(1) was calculated to determine the extent of the variance of proactive ISBs among the departments. The results showed that ICC(1) was .279 ($F_{(54, 155)} = 2.550$, $p < .001$), indicating that 27.9% of the variance in proactive ISBs resided between the departments. Next, we detail the results of the hypothesis testing using this method.

6.1 Hypothesis Testing

RQ1 was addressed by H1–H3. **H1** predicted that employees' proactive motivational state of can-do motivation, represented by security RBSE, would be positively associated with proactive ISBs. This relationship was significant ($\gamma = 0.13$, $p < .01$), thus supporting H1. **H2** predicted that employees' proactive motivational state of reason-to motivation, represented by flexible security role orientation, would be positively associated with proactive ISBs. This relationship was significant ($\gamma = 0.16$, $p < .01$), thus supporting H2. **H3** predicted that employees' proactive motivational state of energized-to motivation, represented by positive affect, would be positively associated with proactive ISBs. This relationship was significant ($\gamma = 0.11$, $p < .01$), thus supporting H3.

RQ2 was addressed by H4–H6. **H4** predicted that supervisory ISec support would be positively associated with employees' proactive motivational states. As **Table 4** shows, supervisory ISec support was positively and significantly associated with employees' security RBSE ($\gamma = 0.15$, $p < .05$), flexible security role orientation ($\gamma = 0.23$, $p < .001$), and positive affect ($\gamma = 0.22$, $p < .01$), respectively. H4 was therefore supported. The findings indicated that employees in departments with stronger supervisory ISec support had stronger proactive motivational states.

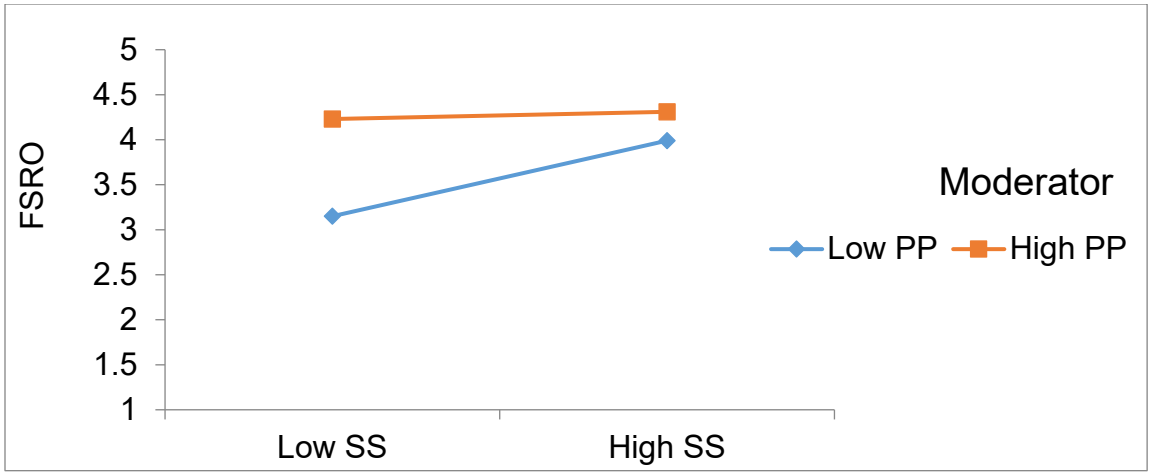
H5 predicted a positive association between the degree to which employees have a proactive personality and the levels of their proactive motivational states. As **Table 4** shows, proactive personality was significantly associated with security RBSE ($\beta = 0.36$, $p < .001$), flexible security role orientation ($\beta = 0.35$, $p < .001$), and positive affect ($\beta = 0.40$, $p < .001$). Thus, H5 was also supported.

H6 predicted that supervisory ISec support would interact with proactive personality to influence proactive motivational states. As **Table 4** and **Figure 2** indicate, proactive personality significantly and negatively moderated the relationship between supervisory ISec support and flexible security role orientation ($\gamma = -0.19$, $p < .05$). This suggests that in employees with a highly proactive personality, the influence of supervisory ISec support on flexible security role orientation was weakened (supporting H6b).

Table 4. Multilevel Path Analysis Results

Variable	Model 1	Model 2	Model 3	Model 4
Intercepts	0.77 (0.72)	1.34* (0.62)	1.16 (0.82)	1.39** (0.45)
Department-level variable				
Supervisory ISec support	0.15* (0.06)	0.23*** (0.05)	0.22** (0.08)	0.11* (0.05)
Multilevel interaction variable				
Supervisory ISec support * Proactive personality	-0.17+ (0.09)	-0.19* (0.08)	0.03 (0.10)	-0.11* (0.05)
Individual-level variables				
Proactive personality	0.36*** (0.07)	0.35*** (0.06)	0.40*** (0.08)	0.13** (0.05)
Security role-breadth self-efficacy				0.13** (0.05)
Flexible security role orientation				0.16** (0.05)
Positive affect				0.11** (0.04)
Control variables				
Job autonomy	0.28*** (0.06)	0.06 (0.05)	0.08 (0.07)	-0.02 (0.04)
Gender	0.17+ (0.09)	0.11 (0.08)	0.20* (0.10)	-0.02 (0.05)
Age	-0.52 (0.64)	-0.16 (0.56)	-0.71 (0.72)	0.11 (0.38)
Department-level pseudo R^2	0.64	0.91	0.52	0.55
Individual-level pseudo R^2	0.26	0.14	0.09	0.34
Total pseudo R^2	0.30	0.26	0.20	0.40

Note. n = 55 (department level); n = 210 (individual level). + p < .10; * p < .05; ** p < .01; *** p < .001; standard errors are reported in parentheses; two-tailed tests were used; Model 1 DV = security role-breadth self-efficacy; Model 2 DV = flexible security role orientation; Model 3 DV = positive affect; Model 4 DV = proactive ISBs.



Note. FSRO = flexible security role orientation; PP = proactive personality; SS = supervisory information security (ISec) support.

Figure 2. Moderation Effect of Proactive Personality

However, the moderation effect of proactive personality on the relationship between supervisory ISec support and security RBSE ($\gamma = -0.17$, $p > .05$) and positive affect ($\gamma = 0.03$, $p > .1$) was not significant (H6a and H6c rejected). H6 was thus only partially supported.

6.2 Post Hoc Mediation and Moderated Mediation Analysis

Although we did not directly hypothesize mediation relationships, our model implies their existence. Thus, we examined the mediating effects and the moderated mediation effects of proactive motivational states. First, using the MLmed SPSS method for multilevel mediation to test these mediating effects (Rockwood & Hayes, 2017), we found that supervisory ISec support significantly influenced proactive ISBs through

increased security RBSE (indirect effect = .06; 95% confidence interval [CI] [0.003, 0.140]). However, the mediating effects of flexible security role orientation (indirect effect = .04; 95% CI [-0.025, 0.115]) and positive affect (indirect effect = .04; 95% CI [-0.016, 0.100]) were not significant.

We also conducted moderated-mediation analyses. We examined the mediating effect of three proactive motivational states on the relationships between supervisory ISec support and proactive ISBs, as moderated by proactive personality. We found that the indirect relationship between supervisory ISec support and proactive ISBs via flexible security role orientation was significantly positive when proactive personality was low (indirect effect = .146; 95% CI [0.0448, 0.2737]). However, the mediating effects of security RBSE (indirect effects = 0.035; 95% CI [-0.0584, 0.1404]) and positive affect (.020; 95% CI [-0.0354, 0.0866]) were not significant under a low level of proactive personality. The results showed that when employees' levels of proactive personality were low, the effect of supervisory ISec support on proactive ISBs was transmitted by reason-to motivation. Previous research has argued that although can-do motivation is a key antecedent of proactive behavior, employees need a powerful reason to behave proactively (Fuller et al., 2012). Thus, when employees lack a powerful reason to behave proactively, supervisors are more likely to motivate employees' engagement in proactive ISBs by increasing their reason-to motivation.

In addition, we found that the indirect relationship between supervisory ISec support and proactive ISBs via security RBSE was significantly positive under a high level of proactive personality (indirect effect = .052; 95% CI [0.0002, 0.1236]). However, the mediating effects of flexible security role orientation (indirect effects = .005; 95% CI [-0.0365, 0.0499]) and positive affect (.031; 95% CI [-0.0111, 0.0853]) were not significant under a low level of proactive personality. The results showed that when proactive personality was high, can-do motivation played a stronger role in transmitting the effect of supervisory ISec support to proactive ISBs. When employees have a highly proactive personality, they are likely to experience strong proactive motivational states. When employees already have a strong reason to act proactively, supervisors can more readily motivate them to engage in proactive ISBs by increasing their can-do motivation.

7 DISCUSSION

Employees' proactive ISBs have become increasingly pivotal in fostering organizational ISec protection. Leveraging a contextualized version of ProMT, we develop an integrated multilevel model to explore how supervisory ISec support interacts with employees' proactive personality and ultimately influences employees' proactive motivational states and proactive ISBs. The empirical results largely support the hypotheses, providing evidence for our theoretical propositions. The results align with Parker et al. (2010) ProMT.

The results of our study suggest that supervisory ISec support and proactive personality interact in security settings. We found that both supervisory ISec support and proactive personality significantly

improve employees' proactive motivational states, which then positively influence employees' proactive ISBs. Our findings highlight the importance of both context-specific variables and individual differences in explaining employees' motivations and behaviors in ISec contexts. Compared to general leadership, we found that supervisory support that specifically targets information security provides a strong and powerful explanation for employees' goal-driving processes. We also found that employees with highly proactive personalities are motivated less by supportive supervisors. Based on the results of this study, we argue that individual differences play a key role in influencing how contextual variables are translated into employees' ISBs. The nonsignificant results for H6a and H6c may indicate that proactive personality and supervisory ISec support operate in a more complex interactive effect on proactive motivational states. When employees' proactive personality levels are high, supervisory ISec support is expected to have a weak or nonsignificant positive effect on proactive motivational states. However, when employees' proactive personality levels are low, the effect of supervisory ISec support on proactive motivational states might not always be significantly positive. For example, according to conservation of resources theory (Hobfoll, 1989), performing proactive behaviors is a resource-depleting process. When employees are skeptical about receiving sufficient support to complete tasks that lie beyond their job requirements, they may develop a sense of vulnerability (Dirks & Skarlicki, 2004; Zhu & Akhtar, 2014). Thus, because they are motivated to conserve resources, employees with low proactive personality levels and low perceived supervisory ISec support may have little confidence or energized motivation to challenge the security status quo.

7.1 Contributions to Research and Theory

Our study makes several valuable contributions to the ISec literature, as highlighted in **Table 5**. *First*, in addressing **RQ1** (via H1–H3), our study complements existing behavioral ISec research by shedding light on employees' proactive ISBs and reframing the core constructs of ProMT within the context of employees' ISBs. This concurs with other scholars' findings that good theorizing in IS relies on a solid foundation of contextualization (Chen et al., 2021; Hong et al., 2014; Luo et al., 2020). In addition, many scholars have argued that it is crucial to differentiate proactive behaviors from compliance behaviors (Grant & Ashford, 2008b; Parker et al., 2010; Parker & Collins, 2010; Parker et al., 2006)) because proactive behaviors have emerged as a vital area of interest in organizational research. Whereas prior ISec research has identified motivational factors, such as self-efficacy (Moody et al., 2018), ISP responsibility (Yazdanmehr & Wang, 2016), and personal norms (Li et al., 2014), we posit that these factors are insufficient to explain employees' proactive ISBs. Therefore, we advance behavioral ISec research by identifying three proactive motivational states that strongly influence employees' proactive ISBs: security role-breadth self-efficacy, flexible security role orientation, and positive affect.

Table 5. Summary of Implications and Contributions

Extant Behavioral ISec Research	Our Approach	Our Contribution

A wealth of research has been conducted on the motivational factors that influence employee compliance. Employees' proactive ISBs, focused on self-initiative, being change oriented, and being future focused, have been understudied.	Introduced proactive ISBs and identified and empirically estimated the effects of three proactive motivational states on proactive ISBs.	• Complements prior behavioral ISec research by identifying proactive ISBs. • Extends ISec research focused on employees' motives by identifying three proactive motivational states.
Primarily considered general variables, such as transformative leadership and top management support as important contextual variables in influencing employees' motivations and ISP compliance.	Developed and investigated the results of a context-specific variable, supervisory ISec support, on three proactive motivational states.	• Enriches ISec research by theorizing and empirically validating the key role of supervisory ISec support in influencing employees' proactive ISBs.
Only a few individual differences are identified and empirically investigated. Analyzed factors influencing employees' ISBs at a single level.	Built an integrated, multilevel research model, including contextual variables as department-level and individual differences as individual-level factors.	• Enhances the understanding of the interplay of individual differences and contextual variables in influencing employees' motivations and ISBs. • Demonstrates the importance of multilevel mechanisms in understanding employees' ISBs.

Second, in addressing **RQ2** (via H4–H6), our study advances behavioral ISec research by unpacking the ways in which contextual factors shape employees' proactive motivational states. Although previous studies have emphasized the importance of contextual factors in employees' motivations and ISBs, they have predominantly focused on general rather than specific variables, such as transformative leadership and top management support (Hu et al., 2012; Posey et al., 2015; Shropshire et al., 2015). By contrast, our study introduces a novel and context-specific variable—namely, supervisory ISec support—which is vital for inducing employees' proactive motivational states, extending ProMT's focus on general leadership. Our findings concur with those of IS studies that have emphasized the influence of contextual factors on employees' attitudes and behaviors (Johnston et al., 2016). These results also align with those of ISec studies that have pointed to the important role that supervisors have in influencing employees' ISBs (Goo et al., 2014; Guan & Hsu, 2020) and have identified the vital role of supervisors in encouraging employees' proactive behaviors (Parker et al., 2006; Wu & Parker, 2017).

Our study also enhances the current understanding of the role of individual differences in influencing employees' proactive motivational states. Previous ISec research emphasizes the importance of individual differences but only focuses on Big Five personality traits (Johnston et al., 2016) and negative affectivity (Posey et al., 2011). We identify a new individual difference of proactive personality and demonstrate that proactive personality interacts with supervisory ISec support to positively influence employees' proactive motivational states. By incorporating supervisory ISec support as a department-level variable and proactive personality as an individual-level variable, our study extends both the ISec literature and ProMT by

constructing an integrated multilevel model. This approach enables us to empirically examine the interaction effect between the two variables. It is noteworthy that the prevailing methodology employed in the existing ISec literature has often overlooked multilevel analyses, primarily focusing on examining the individual-level antecedents of employees' ISBs (Cram et al., 2019; Lowry et al., 2017; Moody et al., 2018); however, substantial ISec research has pointed to the crucial multilevel nature of ISec in organizations (Bélanger & James, 2020; Chul Woo et al., 2020; D'Arcy & Lowry, 2019). Our results demonstrate that department-level processes of supervisory ISec support are foundational for pursuing proactive security goals and emphasize that multilevel mechanisms exert an important effect on employees' ISBs.

7.2 Practical Contributions

Although employees have been regarded as the weakest link in an organization, this study has interesting implications for supervisors seeking to improve organizational security by encouraging employees' engagement in proactive ISBs. Recent studies have demonstrated the positive influence of employees on the effectiveness of organizational ISP. However, encouraging proactive ISBs is a crucial aspect of improving organizational security. Our identification of proactive ISBs and their antecedents provides meaningful guidance regarding what supervisors can do to encourage employees to perform proactive ISBs.

First, our results indicate that individual differences may influence the effects of leadership behavior. That is, proactive personality negatively moderates the relationship between supervisory ISec support and proactive motivational states. Employees with a highly proactive personality are predisposed to have strong proactive motivational states and are less likely to be influenced by their supervisors. In contrast, employees who lack a proactive personality are likely to perform proactive ISBs only when they receive support cues from supervisors. Thus, it is critical for the organization to promote employees' awareness of their personal ability to overcome the costs or risks associated with proactive ISBs. Organizations could develop a variety of strategies to strengthen employees' self-efficacy, such as training them to deal proactively with difficult organizational ISec issues (cf. Hull et al., 2023).

Second, the results imply that at the department level, supervisors can encourage employees to perform proactive ISBs by increasing their can-do, reason-to, and energized-to motivations. In today's dynamic and uncertain security context, unforeseen situations often require employees to be proactive. Encouraging proactive ISBs is thus crucial to addressing unexpected security threats. Performing proactive ISBs can help employees reduce organizational ISec risks. The research is clear: supervisors cannot always positively influence employees through formal controls, and such controls can backfire. Instead, supervisors should encourage employees' self-starting and change-focused behaviors to increase their proactive motivational states and behaviors.

7.3 Limitations and Future Research

This study has several limitations that suggest future research possibilities. *First*, although our findings provide widespread support for our proposed theoretical model, the moderation effects of proactive personality on the relationship between supervisory ISec support and proactive motivational states are nonsignificant, so they need to be further addressed. We encourage researchers to investigate the quadratic relationship between supervisory ISec support and proactive motivational states under different conditions of proactive personality.

Second, although we collected multilevel data and designed multiple ways to reduce CMV, the data are cross-sectional. Future research could collect longitudinal data to further estimate the hypotheses tested in this study. In addition, we used self-reporting measures for employees' proactive ISBs. To verify our findings, future research could use actual behaviors or supervisors' evaluations.

Third, we operationalize three proactive motivational states in an ISec context. We found that only security RBSE exerted a significant mediation effect. The results show that can-do motivation plays a predominant role in transmitting the effects of supervisory support to proactive ISBs. However, the mediation roles of flexible security role orientation and positive affect were not significant. To explain the nonsignificant relationships, future studies could explore the causal ordering between the three operationalized constructs and proactive motivations. Other work-context factors may influence this effect (Parker et al., 2010). For example, previous research has found that time pressure may lead to personal initiative by heightening employees' need for change (Sonnentag, 2003).

Fourth, this study is based on data collected from China, which is considered a strongly collectivistic society. Cultural differences between China and the United States have been identified in ISec and privacy contexts (Lowry et al., 2004; Lowry et al., 2011; Vance et al., 2020). It is possible that culture influences the role of supervisory support. We thus encourage researchers to conduct cross-cultural studies to verify or refute the generalizability of our findings.

7.4 Conclusion

Based on ProMT, we examine the influence of supervisory ISec support and proactive personality on proactive motivational states and proactive ISBs. Based on data collected from 210 employees in 55 departments, we demonstrate that supervisory ISec motivates employees' proactive ISBs by increasing their security RBSE. The data analyses also confirm the moderating role of proactive personality. The findings suggest that supervisors should increase their ISec support to encourage employees' engagement in specific proactive ISBs.

REFERENCES

Alarcon, G., Eschleman, K. J., & Bowling, N. A. (2009). Relationships between personality variables and burnout: A meta-analysis. *Work & Stress*, *23*(3), 244-263.

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security*, *99*(December), Article: 102030. https://doi.org/10.1016/j.cose.2020.102030

Armstrong, J. S., & Overton, T. S. (1977). Estimating nonresponse bias in mail surveys. *Journal of Marketing Research*, *14*(3), 396-402.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, *16*(1), 74-94.

Balozian, P., Leidner, D., & Warkentin, M. (2019). Managers' and employees' differing responses to security approaches. *Journal of Computer Information Systems*, *59*(3), 197-210.

Bandura, A. (1999). A social cognitive theory of personality In L. Pervin & O. John (Eds.), *Handbook of Personality* (pp. 154-196). Guilford Press.

Barclay, D., Higgins, C., & Thompson, R. (1995). The partial least squares (PLS) approach to causal modeling: Personal computer adoption and use as an illustration. *Technology Studies*, *2*(2), 285-309.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2018). Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems*, *19*(8), 308-327.

Baron, R. A. (1990). Environmentally induced positive affect: its impact on self‐efficacy, task performance, negotiation, and conflict. *Journal of Applied Social Psychology*, *20*(5), 368-384.

Bateman, T. S., & Crant, J. M. (1993). The proactive component of organizational behavior: A measure and correlates. *Journal of Organizational Behavior*, *14*(2), 103-118.

Bélanger, F., & James, T. L. (2020). A theory of multilevel information privacy management for the digital era. *Information Systems Research*, *31*(2), 510-536. https://doi.org/10.1287/isre.2019.0900

Bliese, P. D. (2002). Multilevel random coefficient modeling in organizational research: Examples using SAS and S-Plus. In F. Drasgow & N. Schmitt (Eds.), *Advances in Measurement and Data Analysis* (pp. 401-445). Jossey-Bass.

Bolino, M. C., & Turnley, W. H. (2005). The personal costs of citizenship behavior: The relationship between individual initiative and role overload, job stress, and work-family conflict. *Journal of Applied Psychology*, *90*(4), 740-748.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837-864.

Brislin, R. W. (1980). Translation and content analysis of oral and written material. In H. C. Triandis & J. W. Berry (Eds.), *Handbook of Cross-cultural Psychology* (pp. 349-444). Allyn & Bacon.

Brouthers, L. E., Gao, Y., & Napshin, S. (2014). Keiretsu centrality-profits and profit stability: A power dependence perspective. *Journal of Business Research*, *67*(12), 2603-2610.

Brown, D. J., Cober, R. T., Kane, K., Levy, P. E., & Shalhoop, J. (2006). Proactive personality and the successful job search: A field investigation with college graduates. *Journal of Applied Psychology*, *91*(3), 717-726.

Bulgurcu, B., Cavusoglu, H., & 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., & Lowry, P. B. (2019). The adaptive roles of positive and negative emotions in organizational insiders' security-based precaution taking. *Information Systems Research*, *30*(4), 1228-1247. https://doi.org/10.1287/isre.2019.0860

Burns, A. J., Roberts, T. L., Posey, C., Lowry, P. B., & Fuller, B. (2023). Going beyond deterrence: A

middle-range theory of motives and controls for insider computer abuse. *Information Systems Research*, *34*(1), 342-362. https://doi.org/10.1287/isre.2022.1133
Caesens, G., Stinglhamber, F., & Ohana, M. (2016). Perceived organizational support and well-being: A weekly study. *Journal of Managerial Psychology*, *31*(7), 1214-1230.
Chen, G., Farh, J.-L., Campbell-Bush, E. M., Wu, Z., & Wu, X. (2013). Teams as innovative systems: Multilevel motivational antecedents of innovation in R&D teams. *Journal of Applied Psychology*, *98*(6), 1018-1027.
Chen, H., Chau, P. Y., & Li, W. (2019). The effects of moral disengagement and organizational ethical climate on insiders' information security policy violation behavior. *Information Technology & People*, *32*(4), 973-992. https://doi.org/10.1108/ITP-12-2017-0421
Chen, T., Li, F., & Leung, K. (2016). When does supervisor support encourage innovative behavior? Opposite moderating effects of general self-efficacy and internal locus of control. *Personnel Psychology*, *69*, 123-158.
Chen, Y., Galletta, D. F., Lowry, P. B., Luo, X., Moody, G. D., & Willison, R. (2021). Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model. *Information Systems Research*, *32*(3), 1043-1065. https://doi.org/10.1287/isre.2021.1014
Chen, Y., Ning, R., Yang, T., Feng, S., & Yang, C. (2018). Is transformational leadership always good for employee task performance? Examining curvilinear and moderated relationships. *Frontiers of Business Research in China*, *12*(22), 1-28.
Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, *29*(3), 157-188.
Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, *39*(November), 447-459.
Chul Woo, Y., Jahyun, G., & Rao, H. R. (2020). Is cybersecurity a team sport? A multilevel examination of workgroup information security effectiveness. *MIS Quarterly*, *44*(2), 907-931. https://doi.org/10.25300/MISQ/2020/15477
Claes, R., Beheydt, C., & Lemmens, B. (2005). Unidimensionality of abbreviated proactive personality scales across cultures. *Applied Psychology*, *54*(4), 476-489.
Coelho, V. A., & Romão, A. M. (2018). The relation between social anxiety, social withdrawal and (cyber) bullying roles: A multilevel analysis. *Computers in Human Behavior*, *86*(September), 218-226.
Compeau, D., Higgins, C. A., & Huff, S. (1999). Social cognitive theory and individual reactions to computing technology: A longitudinal study. *MIS Quarterly*, *23*(2), 145-158.
Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, *43*(2), 525-554.
Crant, J. M. (1995). The Proactive Personality Scale and objective job performance among real estate agents. *Journal of Applied Psychology*, *80*(4), 532-537.
D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79-98. https://doi.org/10.1287/isre.1070.0160
D'Arcy, J., & Lowry, P. B. (2019). Cognitive‐affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, *29*(1), 43-69. https://doi.org/10.1111/isj.12173
Dasborough, M. T. (2006). Cognitive asymmetry in employee emotional reactions to leadership behaviors. *The Leadership Quarterly*, *17*(2), 163-178.
Deci, E. L., & Ryan, R. M. (1987). The support of autonomy and the control of behavior. *Journal of Personality and Social Psychology*, *53*(6), 1024-1037.
Deci, E. L., & Ryan, R. M. (2000). The" what" and" why" of goal pursuits: Human needs and the self-

determination of behavior. *Psychological Inquiry*, *11*(4), 227-268.
Den Hartog, D. N., & Belschak, F. D. (2012). When does transformational leadership enhance employee proactive behavior? The role of autonomy and role breadth self-efficacy. *Journal of Applied Psychology*, *97*(1), 194-202.
Dirks, K. T., & Skarlicki, D. P. (2004). Trust in leaders: Existing research and emerging issues. In R. M. Kramer & K. S. Cook (Eds.), *Trust and Distrust in Organizations: Dilemmas and Approaches* (Vol. 7, pp. 21-40). Russell Sage Foundation.
Dumas, T. L., & Perry-Smith, J. E. (2018). The paradox of family structure and plans after work: Why single childless employees may be the least absorbed at work. *Academy of Management Journal*, *61*(4), 1231-1252.
Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, *43*(June), 90-110.
Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39-50.
Fredrickson, B. L. (1998). What good are positive emotions? *Review of General Psychology*, *2*(3), 300-319.
Frese, M., & Fay, D. (2001). Personal initiative: An active performance concept for work in the 21st century. *Research in Organizational Behavior*, *23*, 133-187.
Fuller, J. B., & Marler, L. E. (2009). Change driven by nature: A meta-analytic review of the proactive personality literature. *Journal of Vocational Behavior*, *75*(3), 329-345.
Fuller, J. B., Marler, L. E., & Hester, K. (2012). Bridge building within the province of proactivity. *Journal of Organizational Behavior*, *33*(8), 1053-1070.
Gagné, M., & Deci, E. L. (2005). Self‐determination theory and work motivation. *Journal of Organizational Behavior*, *26*(4), 331-362.
Gefen, D., Rigdon, E. E., & Straub, D. (2011). Editor's comments: an update and extension to SEM guidelines for administrative and social science research. *MIS Quarterly*, *35*(2), iii-A7.
Goo, J., Yim, M. S., & Dan, J. K. (2014). A path to successful management of employee security compliance: An empirical study of information security climate. *IEEE Transactions on Professional Communication*, *57*(4), 286-308.
Grant, A. M., & Ashford, S. J. (2008a). The dynamics of proactivity at work. *Research in Organizational Behavior*, *28*(2008), 3-34.
Grant, A. M., & Ashford, S. J. (2008b). The dynamics of proactivity at work. *Research in Organizational Behavior*, *28*, 3-34.
Guan, B., & Hsu, C. (2020). The role of abusive supervision and organizational commitment on employees' information security policy noncompliance intention. *Internet Research*, *30*(5), 1383-1405.
Guhr, N., Lebek, B., & Breitner, M. H. (2019). The impact of leadership on employees' intended information security behaviour: An examination of the full‐range leadership theory. *Information Systems Journal*, *29*(2), 340-362. https://doi.org/10.1111/isj.12202
Guzman, F. A., & Espejo, A. (2019). Introducing changes at work: How voice behavior relates to management innovation. *Journal of Organizational Behavior*, *40*(1), 73-90.
Gwebu, K. L., Wang, J., & Hu, M. Y. (2020). Information security policy noncompliance: An integrative social influence model. *Information Systems Journal*, *30*(2), 220-269. https://doi.org/10.1111/isj.12257
Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate Data Analysis, 7th ed.* Prentice Hall.
Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly*, *20*(3), 257-278.
Hobfoll, S. E. (1989). Conservation of resources: a new attempt at conceptualizing stress. *American*

Psychologist, *44*(3), 513-524.
Hobfoll, S. E., Freedy, J., Lane, C., & Geller, P. (1990). Conservation of social resources: Social support resource theory. *Journal of Social and Personal Relationships*, *7*(4), 465-478.
Hofmann, D. A., Morgeson, F. P., & Gerras, S. J. (2003). Climate as a moderator of the relationship between leader-member exchange and content specific citizenship: Safety climate as an exemplar. *Journal of Applied Psychology*, *88*(1), 170-178.
Hong, W., Chan, F. K., Thong, J. Y., Chasalow, L. C., & Dhillon, G. (2014). A framework and guidelines for context-specific theorizing in information systems research. *Information Systems Research*, *25*(1), 111-136. https://doi.org/10.1287/isre.2013.0501
Hong, Y., Liao, H., Raub, S., & Han, J. H. (2016). What it takes to get proactive: An integrative multilevel model of the antecedents of personal initiative. *Journal of Applied Psychology*, *101*(5), 687-701.
Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management*, *49*(2), 99-110.
Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research*, *26*(2), 282-300. https://doi.org/10.1287/isre.2015.0569
Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615–660.
Hull, D. M., Schuetz, S. W., & Lowry, P. B. (2023). Tell me a story: The effects that narratives exert on meaningful-engagement outcomes in antiphishing training. *Computers & Security*, *129*(June), Article: 103252. https://doi.org/10.1016/j.cose.2023.103252
IBM. (2022). Definitive guide to ransomware 2022. Retrieved December 30, 2022, from https://www.ibm.com/downloads/cas/EV6NAQR4
Ilies, R., & Judge, T. A. (2005). Goal regulation across time: the effects of feedback and affect. *Journal of Applied Psychology*, *90*(3), 453-467.
Jaeger, L., & Eckhardt, A. (2021). Eyes wide open: The role of situational information security awareness for security‐related behaviour. *Information Systems Journal*, *31*(3), 429-472. https://doi.org/10.1111/isj.12317
Jawahar, I. M., Kisamore, J. L., Stone, T. H., & Rahn, D. L. (2012). Differential effect of inter-role conflict on proactive individual's experience of burnout. *Journal of Business and Psychology*, *27*(June), 243-254.
Johns, G. (2018). Advances in the treatment of context in organizational research. *Annual Review of Organizational Psychology and Organizational Behavior*, *5*, 21-46.
Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*, *52*(1), 126-129.
Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549-566.
Johnston, A. C., Warkentin, M., Mcbride, M., & Carter, L. (2016). Dispositional and situational factors: influences on information security policy violations. *European Journal of Information Systems*, *25*(3), 231-251.
Johnston, A. C., Warkentin, M., & Siponen, M. T. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, *39*(1), 113-134.
Kerr, S., & Jermier, J. M. (1978). Substitutes for leadership: Their meaning and measurement. *Organizational Behavior and Human Performance*, *22*(3), 375-403.
Kim, T. Y., Hon, A. H., & Crant, J. M. (2009). Proactive personality, employee creativity, and newcomer outcomes: A longitudinal study. *Journal of Business and Psychology*, *24*(1), 93-103.
LeBreton, J. M., & Senter, J. L. (2008). Answers to 20 questions about interrater reliability and interrater

agreement. *Organizational Research Methods*, *11*(4), 815-852.
Lee, S. H. M., Qureshi, I., Konrad, A. M., & Bhardwaj, A. (2014). Proactive personality heterophily and the moderating role of proactive personality on network centrality and psychological outcomes: A longitudinal study. *Journal of Business and Psychology*, *29*(3), 381-395.
Li, F., Chen, T., Chen, N. Y. F., Bai, Y., & Crant, J. M. (2020). Proactive yet reflective? Materializing proactive personality into creativity through job reflective learning and activated positive affective states. *Personnel Psychology*, *73*(3), 459-489.
Li, H., Sarathy, R., Zhang, J., & Luo, X. (2014). Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. *Information Systems Journal*, *24*(6), 479-502. https://doi.org/10.1111/isj.12037y
Li, M., Liu, Y., Liu, L., & Wang, Z. (2017). Proactive personality and innovative work behavior: The mediating effects of affective states and creative self-efficacy in teachers. *Current Psychology*, *36*(4), 697-706.
Lin, C., Wittmer, J. L., & Luo, X. R. (2022). Cultivating proactive information security behavior and individual creativity: The role of human relations culture and IT use governance. *Information & Management*, *59*(September), Article: 103650. https://doi.org/10.1016/j.im.2022.103650
Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, *86*(1), 114-121.
Lloyd, K. J., Boer, D., Keller, J. W., & Voelpel, S. (2015). Is my boss really listening to me? The impact of perceived supervisor listening on emotional exhaustion, turnover intention, and organizational citizenship behavior. *Journal of Business Ethics*, *130*(3), 509-524.
Locke, E. A., & Latham, G. P. (1990). *A Theory of Goal Setting & Task Performance*. Prentice-Hall, Inc.
Lowry, P., Posey, C., Roberts, T., & Bennett, R. (2004). 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.
Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems*, *27*(4), 163-200.
Lowry, P. B., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. *European Journal of Information Systems*, *26*(6), 546-563.
Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal*, *25*(5), 433-463. https://doi.org/10.1111/isj.12043
Luo, X. R., Li, H., Hu, Q., & Xu, H. (2020). Why individual employees commit malicious computer abuse: A routine activity theory perspective. *Journal of the Association for Information Systems*, *21*(6), 1552-1593. https://doi.org/10.17705/1jais.00646
Luu, T. (2018). Discretionary HR practices and proactive work behaviour: The mediation role of affective commitment and the moderation roles of PSM and abusive supervision. *Public Management Review*, *20*(6), 789-823.
Maas, C. J., & Hox, J. J. (2004). Robustness issues in multilevel regression analysis. *Statistica Neerlandica*, *58*(2), 127-137.
Maas, C. J., & Hox, J. J. (2005). Sufficient sample sizes for multilevel modeling. *Methodology*, *1*(3), 86-92.
Madjar, N., Oldham, G. R., & Pratt, M. G. (2002). There's no place like home? The contributions of work and nonwork creativity support to employees' creative performance. *Academy of Management Journal*, *45*(4), 757-767.
Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1), 285-311.
Morgeson, F. P., & Humphrey, S. E. (2006). The Work Design Questionnaire (WDQ): developing and validating a comprehensive measure for assessing job design and the nature of work. *Journal of*

Applied Psychology, *91*(6), 1321-1339.
Morrison, E. W., & Phelps, C. C. (1999). Taking charge at work: Extrarole efforts to initiate workplace change. *Academy of Management Journal*, *42*(4), 403-419.
NCSAM. (2019). National cybersecurity awareness month. Retrieved April 19, 2021, from https://staysafeonline.org/resource/ncsam19-report/
Niessen, C., Mäder, I., Stride, C., & Jimmieson, N. L. (2017). Thriving when exhausted: The role of perceived transformational leadership. *Journal of Vocational Behavior*, *103*(December), 41-51.
Oettingen, G., Mayer, D., Thorpe, J. S., Janetzke, H., & Lorenz, S. (2005). Turning fantasies about positive and negative futures into self-improvement goals. *Motivation and Emotion*, *29*(4), 237-267.
Oldham, G. R., & Cummings, A. (1996). Employee creativity: Personal and contextual factors at work. *Academy of Management Journal*, *39*(3), 607-634.
Ouyang, K., Cheng, B. H., Lam, W., & Parker, S. K. (2019). Enjoy your evening, be proactive tomorrow: How off-job experiences shape daily proactivity. *Journal of Applied Psychology*, *104*(8), 1003-1019.
Park, J. H., & DeFrank, R. S. (2018). The role of proactive personality in the stressor–strain model. *International Journal of Stress Management*, *25*(1), 44-59.
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. https://doi.org/10.1037/0021-9010.83.6.835
Parker, S. K., Bindl, U. K., & Strauss, K. (2010). Making things happen: A model of proactive motivation. *Journal of Management*, *36*(4), 827-856. https://doi.org/10.1177/0149206310363732
Parker, S. K., & Collins, C. G. (2010). Taking stock: Integrating and differentiating multiple proactive behaviors. *Journal of Management*, *36*(3), 633-662. https://doi.org/10.1177/0149206308321554
Parker, S. K., & Ohly, S. (2008). Designing motivating work. In R. Kanfer, G. Chen, & R. D. Pritchard (Eds.), *Work Motivation: Past, Present, and Future* (pp. 233-384). Routledge.
Parker, S. K., & Sprigg, C. A. (1999). Minimizing strain and maximizing learning: The role of job demands, job control, and proactive personality. *Journal of Applied Psychology*, *84*(6), 925-939. https://doi.org/10.1037/0021-9010.84.6.925
Parker, S. K., & Wall, T. D. (1998). *Job and Work Design: Organizing Work to Promote Well-being and Effectiveness*. Sage.
Parker, S. K., Wall, T. D., & Jackson, P. R. (1997). "That's not my job": Developing flexible employee work orientations. *Academy of Management Journal*, *40*(4), 899–929. https://doi.org/10.5465/256952
Parker, S. K., Williams, H. M., & Turner, N. (2006). Modeling the antecedents of proactive behavior at work. *Journal of Applied Psychology*, *91*(3), 636-652. https://doi.org/10.1037/0021-9010.91.3.636
Petter, S., Straub, D., & 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., & 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., Bennett, R. J., & Roberts, T. L. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security*, *30*(6), 486-497. https://doi.org/10.1016/j.cose.2011.05.002
Posey, C., Roberts, T., Lowry, P. B., Bennett, B., & Courtney, J. (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.
Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179-214.

Quené, H., & Van den Bergh, H. (2004). On multi-level modeling of data from repeated measures designs: A tutorial. *Speech Communication*, *43*(1-2), 103-121.
Quinones, C., & Griffiths, M. D. (2017). The impact of daily emotional demands, job resources and emotional effort on intensive internet use during and after work. *Computers in Human Behavior*, *76*(November), 561-575.
Rockwood, N. J., & Hayes, A. F. (2017). MLmed: An SPSS macro for multilevel mediation and conditional process analysis. Poster presented at the annual meeting of the Association of Psychological Science (APS), Boston, MA.
Rosenbach, W. E. (2018). *Contemporary Issues in Leadership*. Routledge.
Russell, J. A. (2003). Core affect and the psychological construction of emotion. *Psychological Review*, *110*(1), 145-172.
Seo, M. G., Barrett, L. F., & Bartunek, J. M. (2004). The role of affective experience in work motivation. *Academy of Management Review*, *29*(3), 423-439.
Sheldon, K. M., & Elliot, A. J. (1999). Goal striving, need satisfaction, and longitudinal well-being: The self-concordance model. *Journal of Personality and Social Psychology*, *76*(3), 482-497.
Shin, B., & Lowry, P. B. (2020). A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability'that needs to be fostered in information security practitioners and how this can be accomplished. *Computers & Security*, *92*(May), Article: 101761. https://doi.org/10.1016/j.cose.2020.101761
Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*(March), 177-191. https://doi.org/10.1016/j.cose.2015.01.002p
Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217-224.
Sonnentag, S. (2003). Recovery, work engagement, and proactive behavior: A new look at the interface between nonwork and work. *Journal of Applied Psychology*, *88*(3), 518-528.
Tehseen, S., Ramayah, T., & Sajilan, S. (2017). Testing and controlling for common method variance: A review of available methods. *Journal of Management Sciences*, *42*(2), 142-168.
Thomas, J. P., Whitman, D. S., & Viswesvaran, C. (2010). Employee proactivity in organizations: A comparative meta‐analysis of emergent proactive constructs. *Journal of Occupational and Organizational Psychology*, *83*(2), 275-300.
Thompson, J. A. (2005). Proactive personality and job performance: A social capital perspective. *Journal of Applied Psychology*, *90*(5), 1011-1017.
Tucker, S., Chmiel, N., Turner, N., Hershcovis, M. S., & Stride, C. B. (2008). Perceived organizational support for safety and employee safety voice: The mediating role of coworker support for safety. *Journal of Occupational Health Psychology*, *13*(4), 319-330.
Turel, O., Xu, Z., & Guo, K. (2020). Organizational citizenship behavior regarding security: Leadership approach perspective. *Journal of Computer Information Systems*, *60*(1), 61-75.
Vance, A., Lowry, P. B., & Eggett, D. (2015). Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations. *MIS Quarterly*, *39*(2), 345-366.
Vance, A., Siponen, M. T., & Straub, D. W. (2020). Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. *Information & Management*, *57*(4), Article: 103212.
Wall, T. D., & Jackson, P. R. (1997). "That's not my job": Developing flexible employee work orientations. *Academy of Management Journal*, *40*(4), 899–929.
Wang, Z., Xu, S., Sun, Y., & Liu, Y. (2019). Transformational leadership and employee voice: An affective perspective. *Frontiers of Business Research in China*, *13*(2), 1-14.
Warr, P. (1990). The measurement of well-being and other aspects of mental health. *Journal of Occupational Psychology*, *63*(3), 193-210.
Wu, C.-H., & Parker, S. K. (2017). The role of leader support in facilitating proactive work behavior: A

perspective from attachment theory. *Journal of Management*, *43*(4), 1025-1049.
Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, *92*(December), 36-46.
Yazdanmehr, A., Wang, J., & Yang, Z. (2020). Peers matter: The moderating role of social influence on information security policy compliance. *Information Systems Journal*, *30*(5), 1-54. https://doi.org/10.1111/isj.12271
Zhu, J., Feng, G., Liang, H., & Tsui, K.-L. (2023). How do paternalistic leaders motivate employees' information security compliance? Building a climate and applying sanctions. *Journal of the Association for Information Systems*, *24*(3), 782-817. https://doi.org/10.17705/1jais.00794
Zhu, Y., & Akhtar, S. (2014). How transformational leadership influences follower helping behavior: The role of trust and prosocial motivation. *Journal of Organizational Behavior*, *35*(3), 373-392.

APPENDIX A. MEASUREMENT DETAILS

TABLE A.1. Measurement of Constructs, Including Assessment of Reliability and Validity

Construct (CR, AVE) Scaling (Citation)	Item	Loading
Supervisory ISec Support (CR = 0.966; AVE = 0.826); scaling: 1 (strongly disagree) to 7 (strongly agree); from Tucker et al. (2008) and Wu and Parker (2017)	• My supervisor takes the security ideas of employees seriously.	0.846
	• My supervisor is quick to respond to the security issues of employees.	0.908
	• My supervisor encourages employees to voice their concerns about security.	0.908
	• My supervisor is sympathetic and supportive when I am worried or upset about a security problem.	0.956
	• My supervisor gives me encouragement and support when I have a difficult and stressful security task.	0.920
	• My supervisor offers to provide advice or assistance when I need help with a difficult security problem.	0.913
Proactive ISBs (CR = 0.909; AVE = 0.667); scaling: 1 (very unlikely) to 5 (very likely); from Morrison and Phelps (1999) and Hofmann et al. (2003).	• I will try to change the way the job is done to make job-related information more secure.	0.801
	• I will try to institute new work methods that are more effective for ISec protection.	0.821
	• I will try to eliminate redundant or unnecessary procedures to reduce information security risks.	0.796
	• I will try to initiate steps to improve work procedures to strengthen information security.	0.844
	• I will try to correct a procedure or practice with information security risks.	0.820
Security role breadth self-efficacy (CR = 0.882; AVE = 0.654); scaling: 1 (not at all confident) to 5 (very confident); from Parker et al. (2006)	• Present security-related information to a group of colleagues.	0.700
	• Contact people outside the company (e.g., customers) to discuss security problems.	0.790
	• Analyze a long-term security problem to find a solution.	0.857
	• Visit people from other departments to suggest work methods that comply with information security regulations.	0.875
Flexible security role orientation (CR = 0.929; AVE = 0.624); scaling: 1 (to no extent of concern to me) to 5 (to a very large extent of concern to me); from Parker et al. (2006)	• Some essential information systems' security in your area is not being well guaranteed.	0.837
	• Different people in your area are not coordinating their efforts in information security protection.	0.871
	• Security risk level in your area is well above average.	0.775
	• The quality of output of security controls from your area is not as good as it could be.	0.868
	• Other people in your area are not improving their information security skills.	0.751
	• Your work group is not hitting its security protection targets.	0.752
	• The level of security risks in your work area is increasing.	0.803
	• Costs of information security in your area are higher than budget.	0.634
Positive affect (CR = 0.935; AVE = 0.783); scaling: 1 (to a small extent) to 5 (to a very great extent); from Warr (1990)	• Enthusiastic	0.882
	• Excited	0.906
	• Inspired	0.873
	• Joyful	0.877

Construct (CR, AVE) Scaling (Citation)	Item	Loading
Proactive personality (CR = 0.818; AVE = 0.530); scaling: 1 (not at all true of me) to 5 (completely true of me); from Claes et al. (2005)	• If I see something I don't like, I fix it.	0.693
	• No matter what the odds, if I believe in something, I will make it happen.	0.762
	• I love being a champion for my ideas, even against others' opposition.	0.698
	• If I believe in an idea, no obstacle will prevent me from making it happen.	0.755
Job autonomy (CR = 0.865; AVE = 0.686); scaling: 1 (not at all true) to 5 (exactly true); from Morgeson and Humphrey (2006)	• The job gives me a chance to use my personal initiative or judgment in carrying out the work.	0.765
	• The job allows me to make a lot of decisions on my own.	0.975
	• The job provides me with significant autonomy in making decisions.	0.722

REFERENCES FOR APPENDIX A

Claes, R., Beheydt, C., & Lemmens, B. (2005). Unidimensionality of abbreviated proactive personality scales across cultures. *Applied Psychology*, *54*(4), 476-489.

Hofmann, D. A., Morgeson, F. P., & Gerras, S. J. (2003). Climate as a moderator of the relationship between leader-member exchange and content specific citizenship: Safety climate as an exemplar. *Journal of Applied Psychology*, *88*(1), 170-178.

Morgeson, F. P., & Humphrey, S. E. (2006). The Work Design Questionnaire (WDQ): developing and validating a comprehensive measure for assessing job design and the nature of work. *Journal of Applied Psychology*, *91*(6), 1321-1339.

Morrison, E. W., & Phelps, C. C. (1999). Taking charge at work: Extrarole efforts to initiate workplace change. *Academy of Management Journal*, *42*(4), 403-419.

Parker, S. K., Williams, H. M., & Turner, N. (2006). Modeling the antecedents of proactive behavior at work. *Journal of Applied Psychology*, *91*(3), 636-652.

Tucker, S., Chmiel, N., Turner, N., Hershcovis, M. S., & Stride, C. B. (2008). Perceived organizational support for safety and employee safety voice: The mediating role of coworker support for safety. *Journal of Occupational Health Psychology*, *13*(4), 319-330.

Warr, P. (1990). The measurement of well-being and other aspects of mental health. *Journal of Occupational Psychology*, *63*(3), 193-210.

Wu, C.-H., & Parker, S. K. (2017). The role of leader support in facilitating proactive work behavior: A perspective from attachment theory. *Journal of Management*, *43*(4), 1025-1049.