Information Systems Research

Publication details, including instructions for authors and subscription information:
http://pubsonline.informs.org

Exploring Contrasting Effects of Trust in Organizational Security Practices and Protective Structures on Employees' Security-Related Precaution Taking

Malte Greulich; , Sebastian Lins; , Daniel Pienta; , Jason Bennett Thatcher; ; , Ali Sunyaev;

informs
https://pubsonline.informs.org/journal/isre

INFORMATION SYSTEMS RESEARCH
Vol. 35, No. 4, December 2024, pp. 1586–1608
ISSN 1047-7047 (print), ISSN 1526-5536 (online)

Exploring Contrasting Effects of Trust in Organizational Security Practices and Protective Structures on Employees' Security-Related Precaution Taking

Malte Greulich,[a,*] Sebastian Lins,[a] Daniel Pienta,[b] Jason Bennett Thatcher,[c,d] Ali Sunyaev[a,e]

[a] Institute of Applied Informatics and Formal Description Methods, Department of Economics and Management, Karlsruhe Institute of Technology, 76049 Karlsruhe, Germany; [b] Department of Accounting and Information Management, University of Tennessee, Knoxville, Tennessee 37996; [c] Leeds School of Business, University of Colorado Boulder, Boulder, Colorado 80309; [d] Alliance Manchester Business School, University of Manchester, Manchester M15 6PB, United Kingdom; [e] KASTEL Security Research Labs, 76049 Karlsruhe, Germany

*Corresponding author

Contact: malte.greulich@kit.edu, https://orcid.org/0000-0002-2665-3064 (MG); sebastian.lins@kit.edu, https://orcid.org/0000-0001-7480-275X (SL); dpienta@utk.edu, https://orcid.org/0000-0002-0171-6372 (DP); jason.thatcher@colorado.edu, https://orcid.org/0000-0002-7136-8836 (JBT); sunyaev@kit.edu, https://orcid.org/0000-0002-4353-8519 (AS)

Received: October 14, 2021
Revised: October 27, 2022; July 12, 2023
Accepted: September 3, 2023
Published Online in Articles in Advance: January 8, 2024

https://doi.org/10.1287/isre.2021.0528

Copyright: © 2024 The Author(s)

Abstract. Employees' precautionary security behaviors are vital to the effective protection of organizations from cybersecurity threats. Despite substantial security training efforts, employees frequently do not take security precautions. This study draws from trust theory and mindfulness theory to investigate how the bright- and dark-side effects of two conceptualizations of trust in organizational information security impact employees' precaution taking. Insights drawn from a survey of 380 organizational employees suggest that employees who trust their organization's security practices are more committed and less complacent in protecting their organization and more likely to take security precautions. In contrast, we find evidence of the dark-side effect of employees' trust in organizational protective structures by showing that such trust can lead to complacency regarding security. Analyses indicate that security mindfulness mediates the influence of security complacency and security commitment on precaution taking. These results highlight the crucial roles of security commitment, security complacency, and security mindfulness in shaping employees' precaution taking. This study contributes to information security research by providing empirical evidence concerning the simultaneous bright- and dark-side effects of employees' trust in organizational information security, thereby creating valuable opportunities for researchers to theorize about the ways in which trusting beliefs shape employees' security behaviors.

History: Accepted by Paul Pavlou, Senior Editor; Choon-Ling Sia, Associate Editor.

Funding: This work was supported by the Helmholtz Association and KASTEL Security Research Labs [Topic 46.23, Engineering Secure Systems].

Supplemental Material: The online appendix is available at https://doi.org/10.1287/isre.2021.0528.

Keywords: trust • dark-side trust • bright-side trust • information security • mindfulness • commitment • complacency • precaution taking

1. Introduction

The security precautions taken by employees are a cornerstone of organizations' information security (ISec) strategies for protecting their information technology (IT) resources (i.e., information systems (IS) and organizational data) from cybersecurity threats. Precaution-taking behaviors refer to the deliberate actions of employees that protect the organization from security threats (Boss et al. 2009, Burns et al. 2019), including using tools such as multifactor authentication whenever possible or staying informed regarding the latest security threats. Organizations value precaution-taking behaviors because they address the limitations of prescriptive or recommended ISec policies and procedures, which are prone to becoming outdated or irrelevant against emerging threat vectors.

Strategies for encouraging precaution-taking behaviors remain elusive for organizations. Employees often fail to recognize the suspicious features of phishing emails (Wang et al. 2016, Martin et al. 2021), do not adhere to password policies (Siponen et al. 2020), or engage in suspicious behaviors while working remotely (Sarkar et al. 2020, Tessian 2021). Employees exhibit such deficiencies despite organizations' investments in security training programs designed to encourage precaution-taking behaviors (Boss et al. 2009, Burns et al. 2018). Many security breaches result from employees' not taking recommended security precautions, acting in mindless ways, or facilitating cyberattacks themselves (Willison and Warkentin 2013, Jensen et al. 2017, Burns et al. 2019).

To explain why employees remain a source of security breaches, this study draws from trust theory and mindfulness theory to connect employees' perceptions of organizational security and their precaution-taking behaviors. Trust plays a crucial role in organizational ISec because it can lead to employees becoming more committed to security, such as by reducing computer abuse (Lowry et al. 2015) or ISec policy violations (Jeon et al. 2018, Yazdanmehr and Wang 2021). However, trust is not necessarily conducive to organizational ISec behaviors. For instance, trust among coworkers can make employees more complacent about security, causing suboptimal or risky security behaviors, such as leaving one's computer unlocked at work (Karjalainen et al. 2019). Such contrasting effects of trust (i.e., commitment versus complacency) indicate that employees' trust in their organization's security efforts can have bright- and dark-side effects.

Although trust has been studied in the context of ISec research, most studies have focused on the bright side of trust when investigating security-related phenomena, thereby leaving the dark-side effects of trust and its implications unexamined. This problem is prevalent in many fields, as trust researchers have observed that trust studies have tended either to oversimplify trust as leading to positive outcomes or to be biased toward the bright-side effects of trust (Gargiulo and Ertug 2006, Gefen et al. 2008). To provide a more comprehensive understanding of trust in the ISec literature, this study evaluates whether considering the bright- and dark-side effects of trust simultaneously helps researchers explain why some employees take security precautions while others do not. We contend that examining the bright- and dark-side effects of trust can produce a more complete understanding of security-related situations, which are rife with risk and vulnerability, thereby providing an impetus to shift away from a singular perspective on trust that views it as having primarily bright-side effects (Gargiulo and Ertug 2006, Skinner et al. 2014). We ask the following question: *How do the bright-side and dark-side effects of trust influence employees' intentions to take security precautions?*

To answer this question, this study contrasts the effect of two conceptualizations of organizational trust, thereby accounting for different facets of trust in organizational ISec. First, *trust in organizational security practices* reflects an employee's belief that the organization treats its employees well when making security-related demands, for example, by implementing ISec policies or procedures. Second, *trust in organizational protective structures* refers to the extent to which an employee believes that the organization has established protective structures that safeguard the organization from cybersecurity threats. In addition, this study integrates *security commitment* (i.e., feeling more committed to protecting the organization) and *security complacency* (i.e., feeling self-satisfied with the organization's security protections) to operationalize the bright-side and dark-side effects of trust in this context.

To connect trust-related beliefs to precaution-taking behaviors, we draw on mindfulness theory (Thatcher et al. 2018) and prior research highlighting mindfulness mediating role (Dernbecher and Beck 2017, Christensen-Salem et al. 2021). Mindfulness refers to an active and alert state that allows individuals to notice multiple perspectives and to become more aware of their context (Langer 1989). ISec research shows that the state of mindfulness can enable employees to overcome unproductive behavioral security patterns, such as falling for phishing attempts, by encouraging them to take a step back before performing an action (Jensen et al. 2017). Based on a similar argument, ISec researchers have found that the capacity to be mindful is positively associated with precaution-taking behaviors in an organizational security context (Burns 2019).

Insights drawn from the analysis of survey data gathered from 380 organizational employees confirm the simultaneous, contrasting bright- and dark-side effects of trust in the organizational ISec context on precaution-taking behaviors. The results show that employees' trust in organizational security practices leads them to become more committed and less complacent to security, which promotes their intention to take security precautions and makes them more mindful of security, demonstrating the bright-side effects of trust. In contrast, the results indicate that trust in organizational protective structures can lure employees into complacency regarding security, making them less mindful and demonstrating trust's dark side effects. In addition, mediation analyses suggest that security mindfulness fully mediates the influence of security complacency on precaution taking and partially mediates the influence of security commitment in this context. This study contributes to the ISec literature by exploring and verifying the bright- and dark-side effects of trust in organizational ISec, thereby fostering a more complete understanding of these important effects and the role and relevance of trust in ISec research.

2. Precaution Taking, Trust, and Mindfulness Theory in Organizational ISec

2.1. The Relevance of Precaution Taking for Organizational ISec

Precaution taking refers to employees taking deliberate action to secure organizational IT resources against security threats as a result of prescribed or recommended security policies and procedures, as well as individual proactive behaviors (Boss et al. 2009, Burns et al. 2019). For example, an employee might report a suspicious email to comply with a security policy or because the employee is taking discretionary proactive actions with the goal of securing the organization's IT resources (Burns et al. 2019). In the latter aspect, precaution taking includes self-initiated actions taken to protect the organization due to "a desire to attend to the situation proactively through precaution taking" (Burns et al. 2019, p. 1237). Such proactive actions include, for example, the behavior of employees who inform their supervisors of potential security problems or who inform themselves regarding cybersecurity beyond the level that an organization normally expects from its employees.

ISec research has yielded valuable theoretical insights into precaution taking and associated behavioral outcomes (Table 1). ISec studies, among others, show that perceptions of mandatoriness (Boss et al. 2009) and positive and negative emotions influence precaution taking (Burns et al. 2019). Similar works have shown that extrarole security behaviors can contribute to the effectiveness of security policies (Hsu et al. 2015) and have emphasized the importance of protection-motivation behaviors for organizational security (Posey et al. 2013, 2015).

Expanding the knowledge base of ISec researchers and practitioners concerning precaution taking is important for two reasons. First, organizations require employees to be vigilant and attentive when using organizational IT resources—beyond the level that is documented in security policies. Security measures frequently cannot address and mitigate all potential cybersecurity threats. Theorizing about the emergence of precaution taking can help organizations encourage employees to become more engaged with security. This idea is fortified by calls to broaden researchers' theoretical repertoire for studying and explaining precaution-taking behaviors (Burns et al.

Table 1. ISec Research on Precaution Taking and Related Security Behaviors

Study	Sample	Related findings	Theoretical lens
Boss et al. (2009)	Survey of 1,671 medical center employees	Findings suggest that *mandatoriness* (i.e., the individual perception that compliance with security policies is compulsory) effectively motivates individuals to take security precautions.	Control theory
Anderson and Agarwal (2010)	Survey of 594 home computer users (Study 1)	Results suggest that cognitive (i.e., attitude), social (i.e., subjective norms, descriptive norms), and psychological components (i.e., psychological ownership) influence cybercitizens' security-related behavior.	Protection motivation theory
Posey et al. (2013)	Semistructured interviews with 33 participants; survey of 492 participants via an online panel	This paper develops a taxonomy and theory of diversity for protection-motivation behaviors (i.e., organizational insiders' volitional behaviors aimed at protecting relevant organizational IS and information).	Theory of diversity
Hsu et al. (2015)	Survey of a paired sample consisting of 78 managers and 260 employees	Extrarole security behaviors contribute substantially to the effectiveness of ISec policies. Formal control and social control enhance both in- and extrarole security behaviors.	Social control theory
Posey et al. (2015)	Survey of 380 organizational insiders via an online panel	Organizational affective commitment moderates several relationships among various components of protection motivation theory and related outcomes (e.g., protection motivation and past protection-motivation behaviors).	Protection motivation theory
Burns et al. (2019)	Survey of 405 organizational insiders via an online panel	Insiders' psychological capital and psychological distancing mediate the influence of emotions on security-based precaution taking.	Broad-and-build theory
Burns (2019)	Survey of 41 organizational insiders via an online panel	Drawing from organizational mindfulness characteristics of high-reliability organizations, the paper develops a framework and measurement scale for security organizing. The results of a known-group comparison indicate a correlation between high levels of security organizing and high levels of precaution taking.	Organizational mindfulness

2019). Second, the prospect of studying precaution taking aligns with the shift in ISec research and practices that encourage researchers to go beyond the commonly held belief that employees are security's "weakest link" (Mitnick 2003, p. 3). Proponents of this shift argue that incidents inevitably occur and that blaming individuals for such incidents will likely backfire (Pfleeger et al. 2014). Instead, employees' precaution-taking behaviors can be a crucial aspect of organizational security defense and, thus, an important object for researchers' theorizing efforts (Nguyen et al. 2021).

2.2. The Value of Trust Theory to Explain Organizational ISec Behaviors

This study uses trust theory to examine the ways in which employees' trusting beliefs about organizational ISec influence their precaution taking, thereby answering the call to broaden researchers' theoretical repertoire for explaining and predicting precaution-taking behaviors (Burns et al. 2019). Trust generally refers to "a psychological state comprising the intention to accept vulnerability based upon positive expectation of the intentions or behavior of another" (Rousseau et al. 1998, p. 395). Trust facilitates relationships because it mitigates perceptions of risk, uncertainty, and vulnerability (Mayer et al. 1995, Rousseau et al. 1998, Pavlou et al. 2007).

In a work environment, trust pertains to the relationships of employees with, for example, coworkers or teams, a dedicated security function, employer-provided security technologies (e.g., antivirus software, multifactor authentication), or the organization itself. Employees make themselves vulnerable to these trusted parties in their everyday work. For example, employees often trust that an email received from a coworker is safe, that the antivirus software is effective in identifying malicious payloads contained in received documents, or that the organization takes appropriate measures to protect its employees and the data (e.g., social security details, salary information) and does not violate the privacy of employees by implementing exaggerated monitoring practices. Employees might be subjected to penalties or sanctions in case of intentional or unintentional security policy violations (Straub 1990, D'Arcy et al. 2009, Cram et al. 2019), increasing their vulnerability to these trusted parties.

Concerning the positive effects of trust (i.e., its bright side), a meta-review conducted by Colquitt et al. (2007) found trust to be positively associated with organizational citizenship behaviors, such as increased compliance or increased offers to help, and negatively associated with counterproductive behaviors, such as disregarding safety behaviors or tardiness. Table 2 summarizes selected studies on trust that mirror these findings in the ISec context. For example, trust can promote desired precaution-taking behaviors, such as watching over the security behaviors of peers (Yazdanmehr and Wang 2021), or reduce undesired behaviors, such as security policy circumvention (Jeon et al. 2018) and computer abuse (Lowry et al. 2015).

With regard to the negative effects of trust,[1] trust researchers have acknowledged that excessive trust can be "too much of a good thing" (Langfred 2004, p. 385) because of its potential dysfunctional or detrimental effects (McAllister 1997, Gargiulo and Ertug 2006, Workman 2008, Möllering and Sydow 2019). The primary argument supporting this "dark side" of trust is that trust can lead to overreliance, such that individuals rely excessively on a trusted party, which can reduce their vigilance and increase risk-taking and opportunistic behaviors (Workman 2008). Trust hinders the ability of the individual to develop an understanding of the trusted party's actual abilities, is misplaced, or becomes habitual, thereby making individuals oblivious to changing circumstances (Karjalainen et al. 2019, Pienta et al. 2020). For example, empirical evidence indicates that social similarity with a malicious email sender, such as a situation in which a perpetrator uses a familiar coworker's compromised email account, can lead employees to falsely believe that the sender can be trusted, thereby increasing the likelihood of becoming hooked by a phishing email (Workman 2008, Martin et al. 2021). Similarly, employees might become complacent and rely excessively on a dedicated security function within the organization regarding the protection of IT resources (Loch et al. 1992, Stafford 2022). A lack of trust in the relationship between employees and the organization can also have detrimental effects on security, such as increased computer abuse (Posey et al. 2011a) or overreliance on trust cues in emails (Chowdhury et al. 2020).

Although trust researchers have acknowledged in recent decades that trust can have both positive and negative effects (Dirks and Ferrin 2001, Gargiulo and Ertug 2006), it has also been asserted that trust research often suffers from a "pervading optimistic bias" (Gargiulo and Ertug 2006, p. 183) or an "oversimplification of the context in which trust operates" (Gefen et al. 2008, p. 280). Such contentions have led to calls for theoretical approaches that integrate both the bright- and dark-side effects of trust (e.g., Gargiulo and Ertug 2006). In this study, we seek to provide a more integrated and holistic perspective on trust, which can help address the often fragmented and imbalanced perspective on trust found in organizational ISec research and which has the potential to produce fresh and more complete theoretical insights into this pervasive and versatile concept. Next, we outline mindfulness theory's role in connecting employees' trusting beliefs regarding organizational ISec and their precaution-taking behaviors.

2.3. The Role of Security Mindfulness in Connecting Trust-Related Beliefs and Precaution Taking

Mindfulness has been studied across various disciplines (Sutcliffe et al. 2016) as well as in IS research (Dernbecher

Table 2. Related ISec Research on the Bright-Side and Dark-Side Effects of Trust

Study	Sample	Type of study	Trust-related effects
		Panel A. Bright-side effects of trust	
Lowry et al. (2013)	Survey of 202 full-time professionals via an online panel provider	Empirical (quantitative)	Trust in the information quality of online whistle-blowing reporting systems and trust in the authority that receives whistle-blowing reports can positively influence a person's willingness to report an organizational ethical failure (e.g., computer abuse).
Lowry et al. (2015)	Survey of 533 full-time employees from the banking, financial, and insurance industries	Empirical (quantitative)	Organizational trust decreases reactive computer abuse and fully mediates the relationships between fairness perceptions (e.g., explanation adequacy, perceived freedom restrictions) and reactive computer abuse.
Jeon et al. (2018, p. 67)	Multimethod approach including 5 semistructured interviews and a survey of 79 employees	Empirical (qualitative and quantitative)	Informed trust (i.e., "empowering users to override access rules temporarily") can reduce employees' intention to circumvent role-based access controls.
Yazdanmehr and Wang (2021)	Two waves of surveys of 254 employees	Empirical (quantitative)	Perceived trust among coworkers is positively associated with peer monitoring (i.e., actions intended to ensure that the misconduct of one's peers is corrected or reported), which reduces the intention to violate ISec policies.
		Panel B. Dark-side effects of trust	
Workman (2008)	Survey of 612 employees and objective observations	Empirical (quantitative)	Trust (i.e., likeability and credibility) positively influences the frequency with which individuals succumb to social engineering attacks.
Posey et al. (2011a)	Survey of 442 participants via an online panel	Empirical (quantitative)	A lack of attributed trust (i.e., trust that the organization places in employees) can lead to increased computer abuse behaviors on the part of employees.
Karjalainen et al. (2019)	Case study including 47 semistructured interviews	Empirical (qualitative)	Employees frequently encounter a dialectic tension between suspicion and trust regarding the organizational environment and its inherent IS security risks. One interviewee reportedly violated the organization's ISec policy by using a USB device to handle an urgent request from a colleague, trusting that the USB device did not contain malware.
Chowdhury et al. (2020)	35 semistructured interviews with cybersecurity experts, nonsecurity professionals, and private users	Conceptual-empirical (qualitative)	Time pressure can cause users to over-rely on trust cues found in phishing emails or websites, thus making them more vulnerable to social engineering attacks.
Martin et al. (2021)	Survey of 1,161 employees	Empirical (quantitative)	Social similarity (i.e., low social distance) can increase trust, thus increasing the likelihood of individuals becoming hooked by phishing emails from socially close individuals.

and Beck 2017, Thatcher et al. 2018). Mindfulness is generally defined as "a state of alertness and lively awareness" (Langer 1989, p. 138), allowing individuals to notice multiple perspectives and to become more aware of their context (Langer 1989). In this study, we define *security mindfulness* as an employee's state of alertness and lively awareness of the need to protect an organization's IT resources (Thatcher et al. 2018, Pienta et al. 2020).[2] Prior research supports the usefulness of studying the state of mindfulness in the ISec context because mindfulness training enables employees to improve, for instance, their phishing resistance by increasing employees' contextual awareness through active questioning (Jensen et al. 2017).

We employ the concept of mindfulness to connect trust-related beliefs and precaution taking because of its confirmed association with precaution taking (e.g., Burns 2019) and its prescribed role as an intermediary concept in nomological networks (e.g., Dernbecher and Beck 2017). First, mindfulness is particularly germane to precaution taking because it is associated with broadened thinking as well as more flexible and open-minded cognitive processing, thereby addressing the commonly raised need to increase employees' awareness of security issues (Dinev and Hu 2007, D'Arcy et al. 2009, Jaeger and Eckhardt 2021). For example, being mindfully aware of potentially unexpected events can promote proactive behaviors (Curcuruto et al. 2019). Based on a similar argument, ISec researchers have found that the capacity to be mindful is positively associated with precaution-taking behaviors in an organizational security context (Burns 2019). Mindfulness also emphasizes the notion of the future orientation of proactivity (Parker and Collins 2010, Parker and Wu 2014, Curcuruto and Griffin 2016). This notion has been adopted in conceptualizations of IT mindfulness in IS that recognize mindfulness as involving being alert to distinction, which means that users are more likely to recognize discrepancies between their current and future use of IT and seek ways to resolve these discrepancies (Thatcher et al. 2018).

Second, examining mindfulness is useful because IS research highlights the role of mindfulness as an accelerator and mediator (Dernbecher and Beck 2017, Christensen-Salem et al. 2021) and its relation to organizational trust (Nwankpa and Roumani 2014). Research demonstrates that mindfulness can moderate the relationship between diverse theoretical constructs related to IS usage and IT reinvention (Dernbecher and Beck 2017). Specifically, Nwankpa and Roumani (2014) examined the mediating role of mindfulness between employees' organizational trust and enterprise resource planning (ERP) system usage. They argue that organizational trust provides a setting where people do not fear breaking new ground and taking risks, increasing employee mindfulness and, in turn, leading to more frequent use and experimentation with ERP systems (Nwankpa and Roumani 2014). Their findings substantiate the value of examining mindfulness as an important mediator connecting trust-related beliefs to precaution-taking behaviors, as illustrated in our theoretical model in the next section.

3. Theoretical Model and Hypotheses

This study develops a theoretical model of the bright- and dark-side effects of trust on employees' precaution taking (Figure 1). We simultaneously integrate two contrasting effects of trust in this theoretical model, both providing plausible explanations for the impact of trust on precaution taking. First, trust can cause employees to become more committed (Dirks and Ferrin 2002, Tan and Lim 2009), thereby reflecting a bright-side effect of trust. Second, trust can lead to complacency (Gargiulo and Ertug 2006), thereby reflecting the dark-side effect of this factor. To connect these constructs, the model includes security mindfulness as a mediating variable affecting the influence of trust, security commitment, and security complacency on precaution taking. Table 3 provides an overview of the construct definitions used in this study. We explain each part of the model in the following sections.

3.1. Conceptualizing Trust in the Organizational ISec Context

Whereas trust researchers have studied trust in organizational settings in various ways (Dirks and Ferrin 2001), we focus on two conceptualizations of trust that are relevant in an organizational ISec context and that allow us to study the bright- and dark-side effects of trust: (1) trust as a belief regarding the favorability of *organizational security practices* (e.g., Posey et al. 2011b, Lowry et al. 2015, Yazdanmehr and Wang 2021) and (2) trust as a belief concerning the adequacy of *organizational protective structures* (e.g., McKnight et al. 2002, 2011; Pienta et al. 2020).

Trust in organizational security practices refers to employees' belief that the organization acts in favor of or at least not contrary to employees' interests when making security-related demands (Robinson 1996, Nwankpa and Roumani 2014, Lowry et al. 2015). Employees who trust organizational security practices believe that they are treated fairly by the organization, can raise concerns

Figure 1. A Theoretical Model of the Contrasting Effects of Trust on Precaution Taking

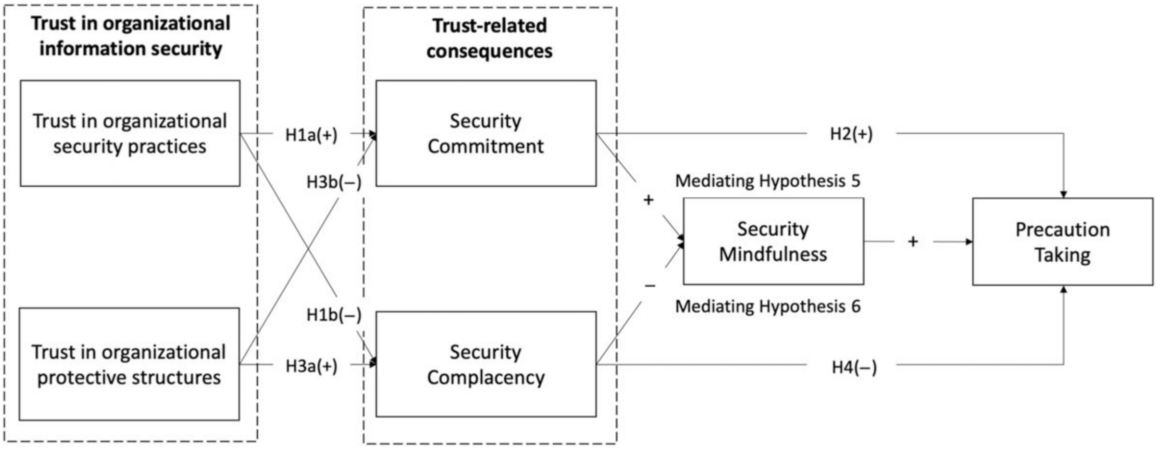

Trust in organizational information security
Trust in organizational security practices
Trust in organizational protective structures
Trust-related consequences
Security Commitment
Security Complacency
H1a(+)
H3b(−)
H1b(−)
H3a(+)
H2(+)
H4(−)
Mediating Hypothesis 5
Mediating Hypothesis 6
+
−
+
Security Mindfulness
Precaution Taking

Table 3. Construct Definitions

Construct	Definition
Precaution taking	Individuals taking actions to secure organizational IT resources against threats as a result of prescribed or recommended security policies and procedures as well as individual proactive behaviors (Boss et al. 2009, Burns et al. 2019)
Trust in organizational security practices	An employee's belief that the organization is acting in favor of or at least not contrary to the employee's interests when making security-related demands (adapted from Robinson 1996, Lowry et al. 2015)
Trust in organizational protective structures	An employee's belief that the organization has put in place necessary impersonal structures to allow the employee to feel safe when working with IS on the job (adapted from McKnight et al. 2002, 2011)
Security commitment	An employee's emotional attachment to, identification with, and involvement in the protection of organizational IT resources (adapted from Meyer and Allen 1991)
Security complacency	An employee's cognitive tendency to become self-satisfied with the organization's security protection against security threats, which leads them to relax their security vigilance (adapted from Parasuraman and Manzey 2010, Markus 2017, Stafford 2022)
Security mindfulness	An employee's state of alertness and lively awareness of the protection of the organization's IT resources (Thatcher et al. 2018, Pienta et al. 2020)

with less fear of repercussions, and know that the organization considers employees' interests when making security-related demands. This conceptualization of trust is in line with the literature on organizational trust, which has portrayed trust as an employee's belief that "organizational action will prove beneficial for employees" (Gilbert and Tang 1998, p. 322), and it follows the stream of ISec literature that has taken the influence of employees' trust in organizational actions into account as an explanatory variable for their security behaviors (e.g., Posey et al. 2011a, Lowry et al. 2015).

Concerning the second conceptualization of trust in ISec, trust in organizational protective structures refers to employees' belief that the organization has put necessary impersonal structures in place to allow them to feel safe when working with IT resources in their jobs (McKnight et al. 2002, 2011). Organizations typically develop, maintain, and update a diversity of complementary security countermeasures, including security policies, Security education, training, and awareness (SETA) programs, and monitoring software as the most prominent examples (D'Arcy et al. 2009). By establishing such protective structures and countermeasures, organizations create a context that safeguards employees from security threats when they use IT resources to accomplish their work. To this end, organizations act as microinstitutions that develop rules, norms, and values that govern organizational and individual behavior (Zucker 1983). This conceptualization corresponds to research that has investigated the impact of impersonal structures on individuals' trusting beliefs and behaviors, such as legal or technical protections (Zucker 1983, McKnight et al. 2002, Lins et al. 2023).

The two conceptualizations of organizational trust used in this study are valuable to examine for two key reasons. First, they parsimoniously allow examination of different trusting beliefs. Trust in organizational security practices uses the trusting beliefs of benevolence, competence, and integrity while also comprising affective beliefs (Nwankpa and Roumani 2014, Lowry et al. 2015). In contrast, trust in organizational protective structures uses the trusting beliefs of structural assurances and situation normality (McKnight et al. 2011), invoking cognitive trusting beliefs. These conceptualizations thereby align with prior studies of trust between employees and organizations: trust in organizational security practices reflecting affective trust and trust in protective structures reflecting cognitive trust. Affective trust in employer and employee relations is established through relational and emotional obligations that involve exchanges that employees see as beneficial beyond the requirements for employment (e.g., additional SETA training, workshops on configuring computers, explanations of countermeasures and how these affect their devices; Macneil 1985). These exchanges often lead to highly salient outcomes (e.g., employees being motivated to do more, such as reporting phishing emails to security) for the organization (Atkinson 2007, Nwankpa and Roumani 2014). In contrast, cognitive trust is established through transactional obligations that involve exchanges that employees see as standard elements of the security required for employment (e.g., required SETA training, multifactor authentication, antivirus protection; Macneil 1985). These obligations lead to low salient outcomes for the organization (e.g., employees doing what is expected or the minimum, such as not opening a phishing email; Atkinson 2007).

Second, we argue that these conceptualizations of trust help capture a broad spectrum of trust's bright-side and dark-side effects that would not be possible to capture by focusing on only one conceptualization. Exploring different conceptualizations of trust accounts for the variety of theoretical views on trust that have been developed (Dirks and Ferrin 2001, Fulmer and Gelfand 2012) and allows us to identify and theorize about contradictory findings and contentions related to trust in the context of organization ISec. In this study, we draw on the literature indicating that the effects of trust can range from the production of commitment to a relationship, a beneficial effect of trust in organizational security practices, to the risk of becoming complacent, a detrimental effect of trust in organizational protective structures (Gargiulo and Ertug 2006). To capture the extremes of trust-related effects, we operationalize the bright- and dark-side effects in terms of *security commitment* and *security complacency*.

Organizational commitment generally refers to the "psychological state that (a) characterizes the employee's relationship with the organization and (b) has implications for the decision to continue or discontinue membership in the organization" (Meyer and Allen 1991, p. 67). ISec research has mostly focused on one component of such commitment, that is, affective organizational commitment (Posey et al. 2015), which is defined as "the employee's emotional attachment to, identification with, and involvement in the organization" (Meyer and Allen 1991, p. 67). *Security commitment* refers to the extent to which an employee is emotionally attached to, identifies with, and is involved in protecting organizational IT resources. Security commitment reflects a contextualized operationalization of affective organizational commitment that aligns with similar notions in the context of committed security attitudes that have been discussed in the ISec literature (Herath and Rao 2009a, Posey et al. 2015). This contextualization also fits with trust in organizational security practices that similarly invoke relational and emotional aspects of trusting relationships, often with positive affect, leading to beneficial outcomes for organizations as employees engage in proactive security (Burns et al. 2019). Therefore, security commitment can help explain why trust in organizational security practices relates to beneficial outcomes.

In contrast, *security complacency* refers to an employee's cognitive tendency to become self-satisfied with the organization's security protection from security threats, which can cause them to relax their security vigilance. This concept aligns with a similar view of complacency found in the automation literature (Parasuraman and Manzey 2010, Markus 2017) and related security research (Stafford 2022). Security complacency captures the notion that employees can become lazy or inert in response to organizational security initiatives (e.g., Guo et al. 2011, Posey et al. 2014) as a result of experiencing a false sense of security. This conceptualization for ISec is important because well-intentioned yet unaware employees present a serious problem for organizations (Stafford 2022). Security complacency is shown to manifest from inherent complacency, or "relaxation of vigilance" when using technology (Stafford 2022, p. 3818); platform complacency, or reliance on technology to mitigate security threats; and social complacency, meaning that security is the responsibility of someone in their social circle rather than theirs directly (Stafford 2022). These manifestations of security complacency are similar to trust in organizational protective structures comprising beliefs about structural assurances and situational normality, or more transactional aspects of trusting relationships, that are shown to reduce employees' security concerns (Pavlou et al. 2007). Accordingly, security complacency helps explain why trust in organizational protective structures can relate to harmful outcomes for organizational security, such as decreased precaution taking.

Importantly, we argue that security commitment and security complacency beliefs might coexist in individuals, with each type of belief leading to different outcomes for security. For example, a highly committed employee might also become complacent, as suggested by Karjalainen et al. (2019), who reported that even a careful employee could occasionally fail to scan a USB device for malware. In turn, complacent employees might misjudge their security responsibilities on occasion but nevertheless feel committed to protecting the organization. Therefore, this study aims to corroborate the contrasting effects of trust on precaution taking via security commitment and security complacency. The following sections develop the hypotheses underlying the theoretical model.

3.2. The Influence of Trust in Organizational Security Practices on Security Outcomes: The Bright Side of Trust

Trust in organizational security practices refers to an employee's belief regarding the favorability of organizational behaviors (Lowry et al. 2015). Suppose employees consider organizational behaviors to be adequate and in the interest of employees. In such a case, they are likely to respond by exhibiting higher levels of affective organizational commitment because the organization demonstrates that it cares for its employees. Previous organizational research has confirmed that employees' trust predicts their affective organizational commitment (Wong et al. 2002, Tan and Lim 2009). Similarly, organizational research has shown that employees' trust in leaders is strongly positively associated with their organizational commitment (Dirks and Ferrin 2002), which aligns with the claim that trust positively influences employees' attitudes toward their workplace (Dirks and Ferrin 2002). Although empirical studies regarding the interplay of trust in organizational security practices and affective organizational commitment remain scarce, extant research has shown that trust, if violated, can reduce commitment to the organization. For instance, hostile or abusive treatment from supervisors can reduce an employee's affective organizational commitment (Guan and Hsu 2020) and increase organization-directed IS misuse (Xu et al. 2022). When employees trust organizational security practices, they believe that the security-related demands of their organizations are reasonable, thus making them more likely to follow prescribed security procedures (Lowry et al. 2015). Employees who trust in organizational security practices are arguably more willing to ask for help with security matters if needed because they expect they will be treated fairly. We conclude the following.

Hypothesis 1a. *Trust in organizational security practices positively influences security commitment.*

Trust in organizational security practices can have an additional bright-side effect by decreasing security complacency. Employees who trust organizational security practices believe that the organization acts in favor of and will prove beneficial for them (Gilbert and Tang 1998, Lowry et al. 2015). Such employees tend to follow the norm of reciprocity (Gouldner 1960), requiring them to return similar benefits to the organization (Coyle-Shapiro and Kessler 2002), such as avoiding potential threats and maintaining the security of their organizations (Liu et al. 2020). These employees may focus on the relational elements of their relationship with the organization in terms of security, such as training, support, and development of security capabilities (Atkinson 2007). Often, employees then engage in high-salience actions such as reporting potential security threats (e.g., phishing emails, violations), completing nonmandatory SETA, and alerting coworkers to best security practices. Thus, organizational trust can act as a catalyst for pro-organizational outcomes, particularly as a hindrance to counterproductive behaviors (Colquitt et al. 2007) such as complacency.

Organizational trust is also shown to promote prosocial compliant behavior (Colquitt et al. 2007) that reduces nonmalicious security violations (Burns et al. 2019) and computer abuse (Lowry et al. 2015), often attributed to apathy, negligence, and loafing (Warkentin and Willison 2009, Cram et al. 2019). Interestingly, recent research has similarly shown that security complacency is a suitable construct for explaining nonmalicious violations (Stafford 2022).

In sum, we propose that trust in organizational security practices will likely lead employees to refrain from behaviors that exacerbate the risk of security threats to the organization. Because security complacency reflects an employee's tendency to relax their security vigilance and related responsibilities, which can harm the organization, we argue that employees will be less inclined to act with complacency if they trust organizational security practices. We therefore posit the following.

Hypothesis 1b. *Trust in organizational security practices negatively influences security complacency.*

We expect security commitment to influence precaution taking based on the arguments that commitment and related attitudes are essential to enacting security behaviors and that commitment drives pro-organizational actions. ISec research has suggested that committed employees may perceive organizational threats as more personally relevant (Posey et al. 2015). The more committed employees are, the greater they feel that threats to the organization are relevant to them. When individuals are committed to the organization, they typically have an interest in staying with the organization (Meyer and Allen 1991). This motivation represents a strong reason for individuals to take security precautions because such behaviors can help reduce the organization's vulnerability to security threats and increase its viability. Therefore, security commitment motivates employees to engage in precaution-taking behaviors that can help mitigate organizational threats, such as cyberattacks. Empirical evidence has also suggested that commitment increases security and compliance-related attitudes, which can increase behavioral compliance intentions (Ifinedo 2014, Aurigemma and Leonard 2015) and security engagement (Davis et al. 2023). Building on these arguments and previous empirical evidence, we posit the following.

Hypothesis 2. *Security commitment positively influences precaution taking.*

3.3. The Influence of Trust in Organizational Protective Structures on Security Outcomes: The Dark Side of Trust

Trust in organizational protective structures consists of two beliefs regarding security-related normality and security-related assurance that are salient to employees. *Perceived security-related normality* refers to the extent to which employees feel secure when working with IS at their job. This facet is associated with the situational normality dimension of institutional trust, which reflects a belief regarding the institutional, organizational context that appears to be stable and commensurate with individuals' expectations (McKnight et al. 2002, 2011). *Perceived security-related assurance* refers to the extent to which employees feel that organizational security measures protect them when working with IT resources at their job. This facet follows the structural assurance dimension of institutional trust, which pertains to the extent to which individuals believe that organizational safeguards and guarantees ensure protection from security threats when individuals use IT resources (McKnight et al. 2002, 2011). For instance, suppose that individuals are confident that their organization safeguards IT resources through appropriate protective mechanisms (e.g., antimalware software, a knowledgeable cybersecurity team, or frequent training on security policies and procedures). Such safeguards may lead employees to focus on the transactional elements of their relationship in terms of security, such as the organization mitigating attacks, warning of attacks, and technological countermeasures performing as expected (Atkinson 2007). In this case, they feel that it is safe to use IT resources because the organization protects them.

Whereas complacency in employee response to security has been noted by ISec researchers (e.g., Loch et al. 1992, Liang and Xue 2009, Stafford 2022), the relationship between complacency and trusting beliefs remains untested. We contend that trust in organizational protective structures plays a key role in influencing security complacency for two reasons.

First, trust has been shown to be a predominant mechanism that reduces ISec concerns in the context of e-commerce (e.g., Gefen et al. 2003, Pavlou et al. 2007). Taking an agency perspective, Pavlou et al. (2007) found that trusting signals and incentives related to structural assurances (e.g., third-party verification of the website) and situational normality (e.g., not price gouging) mitigate security concerns in transactional relationships. We similarly argue that organizational protective structures can send trusting signals and incentives via structural assurances and situational normality to employees. For example, many organizations promote the importance of security, use (advanced) security measures (e.g., antivirus protection, multifactor authentication), demonstrate adherence to regulatory and industry requirements through certification schemes (e.g., third-party verification such as HIPAA (Health Insurance Portability and Accountability Act), ISO/IEC 27001, Payment Card Industry compliance; Lins et al. 2022), and have safe computing policies. Employees might come to trust the effectiveness of these protective structures in protecting the organization (Pienta et al. 2020), especially if they are not aware of recent security breaches or cyberattacks. Because of the ongoing, potentially self-reinforcing perception that "the environment is in proper order and success is likely because the situation is normal or favorable" (McKnight et al. 2002, p. 339), this type of trust can cause employees to rely excessively on organizational protective structures in their work, thus leading to higher levels of security complacency.

Second, trust in organizational protective structures can cause individuals to feel comfortable to the extent that such a feeling limits the cognitive efforts they make to scrutinize the environment (Krishnan et al. 2006, Workman 2008). For instance, antivirus software may block malicious downloads, and antiphishing software may block access to known malicious websites and send warnings about potential risks to employees. Employees familiar with these security technologies and security policies may believe that organizational security technologies are in place to protect them (Stafford 2022). If employees presume that it is normal to rely on organizational protection and that organizational protective structures provide seemingly appropriate safeguards, trust in the organization might reduce individual attention to security and thus increase susceptibility to security attacks (Pienta et al. 2020), for instance, social engineering attacks (Workman 2008). Employees might begin to take organizational protective actions for granted and become complacent regarding the security of IT resources, hence misjudging their own security responsibilities or relaxing their security vigilance. Accordingly, we suggest that trust in organizational protective structures can fuel misconceptions regarding the effectiveness of these structures, thereby luring employees into a state of complacency. We thus posit the following.

Hypothesis 3a. *Trust in organizational protective structures positively influences security complacency.*

Continuing this line of argumentation of trust's adverse consequences, we suggest that trust in organizational protective structures can also adversely impact employees' security commitment. Trust in organizational protective structures focuses on transactional elements of the relationship allowing employees to prioritize other work obligations over security. If employees perceive fewer security threats to their organization because of trust in its protective structures, they may feel less emotionally attached to protecting organizational IT resources. Related trust research substantiates this assumption by showing that cognitive trusting beliefs (i.e., employees having good reasons to feel safeguarded; Lewis and Weigert 1985) also impact their emotions, such as having stronger feelings of security and comfort (Komiak and Benbasat 2006). Often, if employees focus on transactional obligations, they will engage in low-salience actions such as not opening a malicious email or file if warned, completing mandatory security training, and installing security updates only when requested. Employees may, therefore, engage in actions that are more casual and seen as meeting the minimum security requirements in the organization because they feel protected by the organization's structure (Atkinson 2007, Pavlou et al. 2007, Stafford 2022). Hence, although employees might trust in organizational protective structures, this trust can also make them less committed as perceived security concerns and risks decrease. Therefore, we posit the following.

Hypothesis 3b. *Trust in organizational protective structures negatively influences security commitment.*

As security in the organization increases in effectiveness, employees may be complacent in attending to or identifying potential cyberattacks. Individuals have demonstrated a reliance on technology, allowing them to be complacent in certain aspects of their job (Parasuraman et al. 1993). Security complacency manifests in a similar manner, as the literature shows that employees do not feel threats or are not concerned about security because of prevalent security technology at the organization (Stafford 2022). Additional evidence is found in the context of security warnings, where employees become accustomed to these warnings and start disregarding them as a habit (Jenkins et al. 2016). Furthermore, security is often not a priority for employees and groups in organizations, as their work has the highest priority (Herath et al. 2020, Sadok et al. 2020, Sarkar et al. 2020).

When individuals are complacent regarding security, they tend to be less vigilant about the threats inherent to their environment because they are not a concern for them (Parasuraman and Manzey 2010, Markus 2017). Hence, complacent employees seem to misjudge security threats and depend more extensively on existing protective structures in their environment, such as the operating system, for protection from cybersecurity threats (Stafford 2022). Concerning cybersecurity threats in an organizational context, employees are more likely to rely on the organization and established protective structures to address these threats, and, consequently, take fewer or more limited actions themselves. Security complacency seems to eliminate the desire of employees to take proactive actions to protect the organization, which is an essential driver of precaution-taking behaviors (Burns et al. 2019). Tendencies toward complacency connect trust to harmful outcomes for organizational security, such as decreased precaution taking due to misconceptions regarding the security offered by organizational protective structures (Nwankpa and Datta 2023). Following the assertion that more complacent employees are less likely to take security precautions, we posit the following.

Hypothesis 4. *Security complacency negatively influences precaution taking.*

3.4. The Role of Security Mindfulness as a Mediator in the Relationships Between Security Commitment, Security Complacency, and Precaution Taking

Building on mindfulness theory and the related literature, we next examine security mindfulness as a mediating variable in the relationships among security commitment, security complacency, and precaution taking, following the contentions of organizational and IS research that highlight the mediating role of mindfulness (Nwankpa and Roumani 2014, Dernbecher and Beck 2017, Christensen-Salem et al. 2021).

3.4.1. The Mediating Role of Security Mindfulness in the Relationship Between Security Commitment and Precaution Taking. Research connecting commitment and mindfulness remains scarce, especially in the IS domain. In organizational sciences, researchers have argued that affective organizational commitment is likely to promote mindful behaviors (Vogus and Sutcliffe 2012). Relatedly, Choi et al. (2015) found that affective organizational commitment is positively associated with employee work engagement, which refers to a positive mental state in which employees are more energetic and involved in their work (Schaufeli et al. 2002). In such a state, employees are more involved in their work context and are more focused on behaviors that the organization values (Meyer and Allen 1997), a situation that is also salient when individuals engage mindfully with IT (Thatcher et al. 2018). Additionally, organizational research has shown that organizational affective commitment is associated with innovative work behaviors (Jafri 2010), which is also evident when employees engage mindfully with IT because they tend to exhibit a broadened awareness in this context, thus allowing them to develop innovative solutions to problems encountered in their work environment (Langer 2014, Thatcher et al. 2018). In the ISec context, for example, researchers have argued that affectively committed employees perceive organizational threats as more personally relevant (Posey et al. 2015). Hence, the more committed employees are, the greater they feel that the organization's threats are relevant to them, which causes them to become more mindful of security and the need to protect the organization from security threats.

A mindful employee is more likely to recognize the importance of taking security precautions. The findings of previous research have indicated that mindful individuals may examine suspicious emails more attentively (Jensen et al. 2017) and that mindful security organizing is associated with higher precaution taking (Burns 2019). Mindful employees are more likely to recognize discrepancies between their current and potential IT use and find ways of resolving these discrepancies (Thatcher et al. 2018). A mindful employee is more likely to recognize the opportunity to protect organizational IT resources and seek ways to implement these behaviors in their work. Mindful employees may also note alternative uses of a system that can move beyond the purpose intended by the organization (Thatcher et al. 2018). For instance, a mindful employee might use encryption to protect sensitive information in an email to a coworker, even though the ISec policy prescribes the use of encryption only for emails to external parties. Likewise, mindful employees are flexible, curious, and resourceful (Thatcher et al. 2018), aligning well with precautionary actions, such as informing oneself of novel cybersecurity threats. Accordingly, we suggest that security mindfulness mediates the influence of security commitment on precaution taking, which we summarize as follows.

Hypothesis 5. *Security mindfulness mediates the relationship between security commitment and precaution taking.*

3.4.2. The Mediating Role of Security Mindfulness in the Relationship Between Security Complacency and Precaution Taking. Complacent individuals are commonly less suspicious about their environment (Singh et al. 1993, Parasuraman and Manzey 2010) and frequently misjudge the risks associated with a situation, especially when critical events have been avoided successfully in the past (Dillon and Tinsley 2008). A similar argument was also made by Swanson and Ramiller (2004, p. 573), who claimed that a "successful organization may also be prone to fall short in mindfulness—precisely because of its success." Similar tendencies have been acknowledged by ISec researchers, indicating that complacent individuals can develop a false sense of security when working with organizational IS (Loch et al. 1992, Mylonas et al. 2013, Stafford 2022) and underestimate the likelihood or severity of external security threats (Liang and Xue 2009). Complacent individuals are more likely to depend on prior knowledge and previously established structures rather than recognizing changes in the environment (Langer 1989, Wood and Lynch 2002). Hence, we presume that complacent employees are likely to be less mindful regarding security because they are less alert to the events in their environment. Building on the arguments discussed above concerning the positive influence of security mindfulness on precaution taking and the conjectured negative influence of security complacency on security mindfulness, we posit the following.

Hypothesis 6. *Security mindfulness mediates the relationship between security complacency and precaution taking.*

4. Research Method

To test the theoretical model, we conducted a cross-sectional online survey using an online panel provided by Qualtrics. Previous research has confirmed the suitability of online panel data for studying security-related phenomena (Lowry et al. 2016, Burns et al. 2019, Maier et al. 2019). We employed a stratified sampling approach, so we purposefully sampled participants based on two sampling criteria. First, participants were required to have been employed full time for at least one year at a midsize to large company in the United States. This criterion was intended to ensure that employees were sufficiently familiar with their work environment and to reduce cultural biases. Second, participants were required to work occasionally with sensitive data, such as employees' personal information, financial data, or sensitive customer data, thereby ensuring that security was relevant to their jobs. The total panel costs amounted to USD 6,714.03.

4.1. Descriptive Statistics

Qualtrics administered the survey to 744 participants, of whom 607 completed the survey. We included attention-check questions and recorded the time spent on each page to remove respondents who paid insufficient attention to the survey. We removed 121 responses because the answers indicated that the respondents did not meet the sampling criteria. We also removed 106 responses because of failed attention checks or indications that the respondents rushed through the survey. This process resulted in 380 valid responses. This number exceeds the approximate sample size of 146, which we calculated using the tool G*Power (power = 0.950, effect size $f^2 = 0.150$; Faul et al. 2009) and the median sample size of 200 drawn from previous structural equation modeling (SEM) studies (Kline 2016). Among the final participants, 67.63% were women, and 32.11% were men. On average, participants were 50 years old (minimum 20 years old, maximum 76 years old) and reported spending 75.70% of a typical working day using an organization's computer systems, and 76.05% of participants worked with sensitive data approximately half the time or more. The participants worked in various positions in their companies. Most participants held intermediate positions (38.42%), followed by middle management (31.05%), senior management (15.26%), entry level (10.26%), and other positions (5.00%). On average, participants had worked for their current employer for 11.83 years, and worked in the fields of healthcare (21.58%), information technology (10.53%), government (10.53%), academic or education (10.26%), wholesale or retail (9.47%), banking/finance (8.68%), manufacturing (8.68%), or other (20.26%).

4.2. Survey Procedure

The survey consisted of five parts. We first asked questions regarding the sampling criteria noted above (i.e., age, organizational tenure, company size, employment level, and frequency of working with sensitive data), thus allowing the panel provider to filter out participants early in the survey. Subsequently, we provided a short description of the study's context, emphasizing that participants should answer the questions with regard to their current employer, and explained key terminology used in the survey (e.g., security measures, cybersecurity threats). We then measured the dependent variable (i.e., precaution taking), followed by the intermediate variables (i.e., security complacency, security commitment, and security mindfulness) and the antecedent variables (i.e., trust in organizational security practices and trust in organizational protective structures). Subsequently, we collected answers regarding the control variables (i.e., perceived threat, perceived sanctions, perceived mandatoriness, security self-efficacy, disposition to trust, and faith in security technology). Finally, we collected answers pertaining to demographic information, social desirability, and marker items that we collected to estimate common method bias (CMB). We pretested the survey procedure through consultation with eight faculty members and incorporated their feedback.

4.3. Survey Measures

We used or adapted previously validated scales to measure the constructs included in our survey (Straub 1989). To measure precaution taking, we adopted the scales developed by Boss et al. (2009). Trust in organizational security practices was measured using items that we adapted from Robinson (1996) and Schoorman et al. (2007). Trust in organizational protective structures was measured using the two sub dimensions of security-related situational normality and security-related structural assurances, which we adapted from items reported by McKnight et al. (2002, 2011). We adopted the operationalization of security mindfulness from Thatcher et al. (2018) and the operationalization of security commitment from Allen and Meyer (1990) and Herath and Rao (2009b). The items used to measure security complacency were adapted from the complacency potential scale developed by Merritt et al. (2019). Additionally, we collected theoretically relevant control variables to test the robustness of our predictions (Spector and Brannick 2011). The measures are presented in Online Appendix A.

In addition to relying on previously validated items to measure the constructs, we performed additional measurement instrument robustness checks (Online Appendix B). First, 20 faculty members participated in a modified card-sorting procedure (Moore and Benbasat 1991). We asked them to rate on a five-point Likert scale how well each item corresponds to our six key constructs. The results show that faculty members rated a significantly higher fit of the items to their corresponding constructs in comparison with the remaining constructs (e.g., the lowest average fit of items to their theoretical constructs was 3.9 on a five-point Likert scale for precaution taking). Second, we conducted a matching exercise (Thatcher et al. 2018) with 93 participants using the panel provided by Amazon Mechanical Turk (MTurk). We presented each participant with a list of contextualized items of a specific construct and asked them to map each item to the original items used in prior research. We found that the participants, on average, correctly mapped 83% of our contextualized items to the original items of prior research, providing support that participants viewed our contextualized measures and the original items as very similar (Landis and Koch 1977, Thatcher et al. 2018). We also asked participants what they thought when reading example items to assess whether our items were interpreted as intended. Finally, we conducted a pilot test featuring 104 participants acquired using MTurk and assessed construct reliability, convergent validity, and discriminant validity.

4.4. Data Analysis

We used IBM SPSS Statistics (version 27) and IBM SPSS AMOS (version 27), a covariance-based SEM software, to analyze the data. To validate our measurement model, we followed a two-step approach. First, we tested the measurement items for univariate normality. One precaution-taking item (PREC3) exhibited the highest skewness value (−2.368) and the highest kurtosis value (8.067). The highest skewness value was below the acceptable threshold of three, and the highest kurtosis value was below the acceptable threshold of 10, thus suggesting that the item distributions were not severely nonnormal (Kline 2016).

Second, we conducted a confirmatory factor analysis (CFA) using AMOS. We modeled trust in organizational protective structures as a parcel construct consisting of items pertaining to security-related situational normality and security-related structural assurances. All items loaded significantly and highest on their theoretical construct (see Online Appendix A). To assess model fit, we used the chi-squared (χ^2)/degrees of freedom (df) ratio, the root mean square error of approximation (RMSEA), the comparative fit index (CFI), and the standardized root mean square residual (SRMR). The CFA model indicated an acceptable fit with the data ($\chi^2/\text{df} = 1.780$, RMSEA = 0.045, CFI = 0.927, SRMR = 0.057), meeting common thresholds for acceptable model fit ($\chi^2/\text{df} < 3$, CFI > 0.900, RMSEA and SRMR < 0.080; Hu and Bentler 1999, Gefen et al. 2011).

We also assessed the reliability and convergent validity of the reflective constructs and examined their discriminant validity. The average variance extracted (AVE) was higher than the threshold of 0.500 (Fornell and Larcker 1981; Table 4), except for our control variable social desirability (AVE = 0.473). Because social desirability slightly falls below the 0.500 threshold but has a composite reliability (CR) of 0.726, we kept social desirability in our model (cf. Fornell and Larcker 1981). Each construct's CR value was above 0.700, thus demonstrating good internal consistency (Nunnally 1978). All indicators satisfied the minimum loading requirements (significance and load value) between the indicator and its latent construct, thereby exhibiting satisfactory convergent validity. The heterotrait–monotrait (HTMT) ratios of correlations (Table 5) were below the threshold of 0.850 for all constructs (Henseler et al. 2015), indicating no problems with discriminant validity. The square root of each construct's AVE exceeded the interconstruct correlations (Table 4), except for trust in organizational security practices, which was correlated with trust in organizational protective structures at 0.729, slightly above the square root of the AVE, which was 0.721. To further test the discriminant validity, we compared the covariances between models that either freely estimated the covariance between the two constructs or constrained it to one (Wright et al. 2012). The chi-square differences between these models were significant (unconstrained model, $\chi^2 = 146.802$ (34 df); constrained model, $\chi^2 = 202.231$ (35 df); $\Delta\chi^2 = 55.429$, $p < 0.001$). These results support the discriminant validity of the constructs. Additionally, we examined variance inflation factor (VIF) values that can indicate pathological multicollinearity (Kline 2016). All VIF values were lower

Table 4. AVE, CR, and Interconstruct Correlations

Construct	AVE	CR	1	2	3	4	5	6	7	8	9	10	11	12
1. *Precaution taking*	0.573	0.869	**0.757**											
2. *Security mindfulness*	0.626	0.907	0.622	**0.791**										
3. *Security complacency*	0.531	0.850	−0.247	−0.284	**0.729**									
4. *Security commitment*	0.572	0.842	0.645	0.459	−0.226	**0.756**								
5. *Trust in practices*	0.520	0.812	0.454	0.298	−0.006	0.714	**0.721**							
6. *Trust in structures*	0.665	0.922	0.321	0.122	0.144	0.561	0.729	**0.815**						
7. *Security self-efficacy*	0.596	0.815	0.523	0.508	−0.213	0.602	0.512	0.468	**0.772**					
8. *Perceived threat*	0.755	0.860	0.154	0.050	−0.024	0.241	0.179	0.119	0.205	**0.869**				
9. *Perceived sanctions*	0.657	0.851	0.294	0.212	−0.094	0.282	0.273	0.186	0.282	0.292	**0.811**			
10. *Social desirability*	0.473	0.726	0.398	0.335	−0.027	0.450	0.472	0.461	0.250	0.063	0.223	**0.688**		
11. *Disposition to trust*	0.798	0.922	0.044	0.100	0.089	0.231	0.248	0.247	0.138	0.042	−0.034	0.254	**0.894**	
12. *Faith in security measures*	0.690	0.869	0.316	0.291	0.092	0.506	0.585	0.589	0.485	0.165	0.178	0.435	0.289	**0.830**

Note. Diagonal bold numbers show the square roots of the AVE.

than the threshold of five (Kock and Lynn 2012; i.e., the highest VIF value is 2.360), thus suggesting that this is not the case.

4.5. Common Method Bias Assessment

The survey used procedural and statistical remedies to reduce CMB (Podsakoff et al. 2003). First, we told participants that their answers would be anonymized, that they should take the time to answer the questions carefully and honestly, and that there were no right or wrong answers. Furthermore, we randomized the order of questions, used validated scales drawn from the literature, randomized items, and used temporal and proximal separation (i.e., on different pages) of the measurements for independent and dependent variables.

We used three statistical techniques to assess CMB. First, we examined item correlations (Lindell and Whitney 2001, Liang et al. 2019). We used the second-smallest positive correlation as a cautious CMB estimate (i.e., $r = 0.0017$ between PREC3 and DISP3) to calculate CMB-corrected correlations and significances. The pattern of significance remained unchanged, thus suggesting that CMB did not substantially affect our data. Second, we added an unmeasured latent common method factor to the CFA model and allowed all items to load on their latent theoretical construct as well as the method factor (Podsakoff et al. 2003). For identification purposes, we constrained item loadings on the method factor to be equal. The change in CFI (ΔCFI = 0.0004) was below the commonly established threshold of 0.010 (Cheung and Rensvold 2002), thus suggesting that the models were only marginally different. Third, we used the CFA marker technique (Williams et al. 2010) with a measured latent marker variable (Chin et al. 2013). We compared a baseline model in which item loadings to the marker variable were constrained to zero with a model that imposed equality constraints (Williams et al. 2010). The change in CFI (ΔCFI = 0.008) was also below the 0.010 threshold. In summary, these results indicate that CMB does not seem to have been a major concern for our research.

5. Results

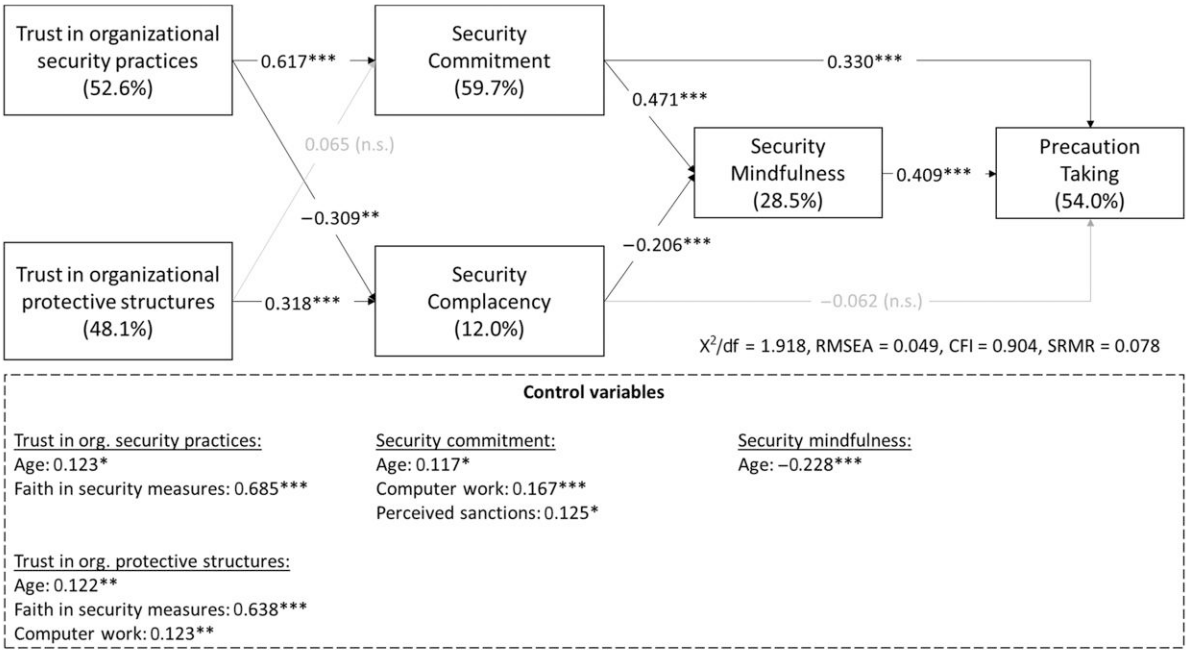
5.1. Hypothesis Testing

Next, we assessed the significance of the structural path estimates in our theoretical model using the AMOS software. Figure 2 and Table 6 present the model testing results. The model explains 54.0% of the variance in precaution taking, 28.5% of the variance in security mindfulness, 59.7% of the variance in security commitment,

Table 5. HTMT Results

Construct	1	2	3	4	5	6	7	8	9	10	11	12
1. *Precaution taking*												
2. *Security mindfulness*	0.650											
3. *Security complacency*	0.261	0.280										
4. *Security commitment*	0.659	0.508	0.218									
5. *Trust in practices*	0.466	0.361	0.008	0.706								
6. *Trust in structures*	0.332	0.172	0.156	0.547	0.719							
7. *Security self-efficacy*	0.545	0.547	0.204	0.633	0.529	0.495						
8. *Perceived threat*	0.177	0.06	0.026	0.242	0.180	0.113	0.215					
9. *Perceived sanctions*	0.310	0.264	0.091	0.296	0.302	0.194	0.307	0.290				
10. *Social desirability*	0.428	0.386	0.028	0.475	0.517	0.478	0.269	0.054	0.246			
11. *Disposition to trust*	0.053	0.110	0.094	0.240	0.249	0.254	0.147	0.041	0.023	0.267		
12. *Faith in security measures*	0.329	0.324	0.097	0.496	0.582	0.590	0.519	0.170	0.188	0.456	0.289	

Figure 2. Model Testing Results


Trust in organizational security practices (52.6%)
0.617***
Security Commitment (59.7%)
0.330***
0.471***
0.065 (n.s.)
Security Mindfulness (28.5%)
0.409***
Precaution Taking (54.0%)
−0.309**
Trust in organizational protective structures (48.1%)
0.318***
Security Complacency (12.0%)
−0.206***
−0.062 (n.s.)
X²/df = 1.918, RMSEA = 0.049, CFI = 0.904, SRMR = 0.078
Control variables
Trust in org. security practices:
Age: 0.123*
Faith in security measures: 0.685***
Security commitment:
Age: 0.117*
Computer work: 0.167***
Perceived sanctions: 0.125*
Security mindfulness:
Age: −0.228***
Trust in org. protective structures:
Age: 0.122**
Faith in security measures: 0.638***
Computer work: 0.123**

Notes. Nonsignificant (n.s.) control variables ($p \geq 0.050$) are not shown. *$p \leq 0.050$; **$p \leq 0.010$; ***$p \leq 0.001$.

12.0% of the variance in security complacency, 52.6% of the variance in trust in organizational security practices, and 48.1% of the variance in trust in organizational protective structures.

5.2. Direct Effects

Hypotheses 1a–4 pertain to the direct effects in the model. The standardized path coefficient between trust in organizational security practices and security commitment was significant ($\beta = 0.617$, $p \leq 0.001$). The standardized path between trust in organizational security practices and security complacency was significant ($\beta = -0.309$, $p \leq 0.010$). Thus, Hypotheses 1a and 1b are supported. Hypothesis 2 focuses on the influence of security commitment on precaution taking. The significant positive path coefficient ($\beta = 0.330$, $p \leq 0.001$) supports

Table 6. Summary of Hypothesis Testing Results

Hypothesis (direction)	β coefficient	p-value	Supported?
	Panel A. Direct effects		
H1a: Trust in org. security practices → Security commitment (+)	0.617	≤0.001	Yes
H1b: Trust in org. security practices → Security complacency (−)	−0.309	0.002	Yes
H2: Security commitment → Precaution taking (+)	0.330	≤0.001	Yes
H3a: Trust in org. protective structures → Security complacency (+)	0.318	≤0.001	Yes
H3b: Trust in org. protective structures → Security commitment (−)	0.065	0.228	No
H4: Security complacency → Precaution taking (−)	−0.062	0.180	No
	Panel B. Mediation effects		
	Coefficient [CIs]	p-value	Supported?
H5: Security commitment → Security mindfulness → Precaution taking	*ab* = 0.166 [0.106, 0.253] *c* = 0.285 [0.109, 0.502]	*ab*: ≤0.001 *c*: ≤0.001	Yes (complementary mediation)
H6: Security complacency → Security mindfulness → Precaution taking	*ab* = −0.055 [−0.107, −0.020] *c* = −0.041 [−0.110, 0.023]	*ab*: ≤0.001 *c*: 0.205	Yes (indirect-only mediation)

Notes. H, Hypothesis. Confidence intervals (CIs) and p-values for mediation effects were obtained using the bootstrapping method (5,000 repetitions, 95% bias-corrected CIs). The letter "*a*" denotes the path between each independent and mediating variable, "*b*" indicates the path between the mediating and dependent variable, and "*c*" represents the path between the independent and dependent variables.

Hypothesis 2. Hypothesis 3a considers the direct influence of trust in organizational protective structures on security complacency, which was found to be positive and significant ($\beta = 0.318$, $p \leq 0.001$), thereby supporting Hypothesis 3a. Hypothesis 3b considers the direct influence of trust in organizational protective structures on security commitment, which was nonsignificant ($\beta = 0.065$, $p = 0.228$), not supporting Hypothesis 3b. Last, Hypothesis 4 pertains to the direct negative effect of security complacency on precaution taking. The path coefficient was not significant ($\beta = -0.062$, $p = 0.180$), thereby not supporting Hypothesis 4. Hence, the results support all but two hypothesized direct effects. We controlled for several possible confounding variables to test the robustness of our model (see Online Appendix C).

5.3. Mediation Effects

Hypotheses 5 and 6 pertain to the hypothesized mediation effects included in the theoretical model. To obtain the estimates for these mediation effects, we used SPSS AMOS "estimands" function with bootstrapping (5,000 repetitions, 95% bias-corrected confidence intervals), as recommended by MacKinnon et al. (2004). We calculated the product of the unstandardized path estimates between the independent variable and the mediator variable (path *a*) and between the mediator variable and the dependent variable (path *b*), and we assessed the significance of the direct effect between the independent and the dependent variable (path *c*; Zhao et al. 2010). Hypothesis 5 focuses on the mediating influence of security mindfulness in the relationship between security commitment and precaution taking. The product term for the indirect effect on the relationship between security commitment and precaution taking via security mindfulness was significant and positive ($ab = 0.166$, $p \leq 0.001$, bias-corrected confidence interval [0.106, 0.253]). The direct effect of security commitment on precaution taking was also significant ($c = 0.285$, $p \leq 0.001$, [0.109, 0.502]), thus suggesting a complementary mediation (i.e., both effects point in the same direction; Zhao et al. 2010), and thereby Hypothesis 5.

Hypothesis 6 focuses on the mediating influence of security mindfulness in the relationship between security complacency and precaution taking. The product term for the indirect effect is negative and significant and ($ab = -0.055$, $p \leq 0.001$, [−0.107, −0.020]), whereas the direct effect is nonsignificant ($c = -0.041$, $p > 0.050$, [−0.110, 0.023]). These results support Hypothesis 6 and indicate an indirect-only mediation (Zhao et al. 2010). Hence, the results support all hypothesized mediation effects.

5.4. Post Hoc Analyses

In the post hoc analyses, we analyzed the effect sizes of the independent variables predicting precaution taking (Online Appendix D). The results indicated a small effect size of the influence of security commitment on the explained variance in precaution taking ($\Delta R^2 = 0.065$, $f^2 = 0.141$) and a medium effect size of the influence of security mindfulness ($\Delta R^2 = 0.103$, $f^2 = 0.224$).

Next, we examined the mediating effects of security commitment and security complacency on the relationships among trust in organizational security practices, trust in organizational protective structures, and security mindfulness. The product term for the indirect effect between trust in organizational security practices and security mindfulness via security commitment was significant and positive ($ab = 0.476$, $p \leq 0.001$, [0.233, 0.927]). The direct effect of trust in organizational security practices on security mindfulness was nonsignificant ($c = 0.270$, $p > 0.050$, [−0.178, 0.721]), thus suggesting an indirect-only mediation.

The product term for the indirect effect on the relationship between trust in organizational protective structures and security mindfulness via security complacency was significant and positive ($ab = -0.083$, $p < 0.050$, [−0.201, −0.015]), whereas the direct effect of trust in organizational protective structures on security mindfulness was also significant ($c = -0.265$, $p < 0.050$, [−0.529, −0.044]). These results indicate a complementary mediation relationship. Hence, trust in organizational protective structures has a significant negative direct effect on security mindfulness beyond its indirect influence via security complacency, thus providing further support for the dark-side effect of trust. In contrast, the effect of trust in organizational security practices is completely mediated by security commitment.

We also tested the direct effects of trust in organizational security practices and trust in organizational protective structures on precaution taking. The results indicate that the effect of trust in organizational security practices on precaution taking is nonsignificant ($c = -0.050$, $p > 0.050$, [−0.427, 0.272]), thereby suggesting that the effect is fully mediated by security commitment. Similarly, the effect of trust in organizational protective structures has no direct significant relationship ($c = 0.006$, $p > 0.050$, [−0.221, 0.202]) with precaution taking, thus suggesting that this effect is fully mediated by security complacency and security mindfulness.

Finally, we analyzed an alternative model (Online Appendix E) to account for reverse causality between security commitment and security mindfulness as well as security complacency and security mindfulness. To do so, we developed an atheoretical alternative model (Khuntia et al. 2021) that had security mindfulness as an antecedent to security commitment and complacency and direct paths from trust in organizational security practices and trust in organizational protective structures to security mindfulness. Additionally, direct paths were modeled from security commitment, complacency, and mindfulness to precaution taking. The proposed theoretically driven research model (Figure 1) has a better overall fit than the alternative model, indicating that the alternative model is misspecified ($\chi^2/\text{df} = 2.004$, $\text{RMSEA} = 0.051$, $\text{CFI} = 0.895$, $\text{SRMR} = 0.092$). Additionally, the variance explained by mindfulness decreases from 28.5% to 20.8%, that explained by security commitment decreases from 59.7% to 43.5%, and that explained by complacency only slightly increases from 12.0% to 14.2%. The variance explained by precaution taking has a minimal change of 0.2%. Empirically, the alternative model's fit and variance explained provide support for our theoretically driven proposed research model rather than the atheoretical alternative model.

6. Discussion

This study develops and tests an integrated theoretical model that focuses on the ways in which the bright- and dark-side effects of trust influence employees' intentions to take security precautions in the context of organizational ISec. Concerning the bright-side effects, the results show that trust in organizational security practices positively influences security commitment, which predicts precaution taking, either directly or indirectly, via its influence on security mindfulness. In addition, analyses suggest that trust in organizational security practices also reduces security complacency, which constitutes an additional bright-side effect.

With regard to the dark-side effects of trust, we find two ways in which trust in organizational protective structures can interfere with employees' intentions to take security precautions. First, trust in organizational protective structures can encourage employees to become complacent, which inhibits their mindfulness in the context of security issues and reduces their intention to take security precautions. Second, employees' trust in organizational protective structures also has a direct negative influence on their security mindfulness, which has the same adverse consequences on precaution taking. These insights are particularly germane to the discourse concerning the bright- and dark-side effects of trust in organizational ISec, thereby offering promising implications for research.

6.1. Implications for Research

Our study makes several notable contributions to the ISec and IS trust literature. First, this study offers nuanced insights into the role of trust in organizational ISec by simultaneously studying the bright-side and dark-side effects of trust within an integrated model. Our work thereby extends previous trust research in ISec that focused on either trust's bright-side effects (e.g., Lowry et al. 2015, Jeon et al. 2018) or dark-side effects (e.g., Workman 2008, Posey et al. 2011a). Specifically, we empirically verify that security commitment and security complacency represent theoretically grounded manifestations of the bright- and dark-side effects of trust in the context of organizational ISec. By examining these contrasting bright- and dark-side effects, we demonstrate the viability of taking a more complete and integrated approach to theorizing trust, as has been recommended in the trust literature (Gargiulo and Ertug 2006, Schoorman et al. 2007, Gefen et al. 2008).

Second, our study suggests that security commitment plays a crucial role as a bright-side effect of trust in organizational ISec. Our findings indicate that employees who are committed to security are more likely to take security precautions and are also more mindful of security. These are vital findings because they empirically validate security commitment as a bright-side effect of trust in organizational ISec. By offering empirical evidence concerning the relationship between security commitment and precaution taking, a desirable security behavior, we extend the findings of previous ISec studies, which have primarily used commitment as a way of explaining undesirable security behaviors (Posey et al. 2011a, Lowry et al. 2015). Our study also demonstrates that a contextualized operationalization of commitment for ISec can have substantial predictive and explanatory power, which underlines the importance of contextual explanations for phenomena related to ISec (Hong et al. 2014, Karjalainen et al. 2019).

Third, we examined security complacency as a dark-side effect of trust in organizational ISec. Security complacency is a novel concept that is important to ISec researchers because it captures a more complete understanding of nonmalicious behaviors (Stafford 2022) than mere apathy or laziness, which often have been identified as employees' response to organizational security initiatives (e.g., Guo et al. 2011, Posey et al. 2014). Security complacency serves as an explanation for why employees facilitate security breaches with no intended malice. However, ISec researchers have not empirically tested the role of complacency as a dark-side effect of trust in organizational ISec. Drawing from existing psychometric research on complacency in the automation literature (Singh et al. 1993, Parasuraman and Manzey 2010) and related security research (Stafford 2022), this study provides empirical support for the role of complacency as a manifestation of a dark-side effect of trust in organizational ISec (Gargiulo and Ertug 2006) because it prevents employees from acting mindful about security. These insights regarding the role of complacency also align well with previous ISec research, which has shown that employees' feelings of happiness regarding the protection of the organization are positively associated with their efforts to detach themselves from potentially threatening situations, which reduces their intentions to take security precautions (Burns et al. 2019). By providing evidence to support the significance of security complacency, we provide researchers with an additional way of understanding employees' security beliefs and behaviors.

Fourth, our study also provides insights into the ways in which security commitment and security complacency are related to different conceptualizations of trust in organizational ISec, namely, trust in organizational security practices and trust in organizational protective structures. Previous research has shown that trust can have different outcomes, depending on the type of trust or level of analysis (Dirks and Ferrin 2001; McKnight et al. 2002, 2011). Our results highlight that employees' trust in organizational security practices increases their security commitment and decreases their security complacency. These bright-side effects reveal the importance of creating a trusting security climate in organizations that empowers employees to deal with security with the organization's help. On a more critical note, we provided empirical evidence indicating that trust in organizational protective structures can cause employees to become complacent regarding security. Thus, our study emphasizes that it is essential to understand where individuals place their trust in the context of organizational ISec because such trust can have both bright- and dark-side effects.

Fifth, previous ISec research has acknowledged the need to broaden ISec researchers' theoretical repertoire regarding understanding security behaviors (Willison and Warkentin 2013, Burns et al. 2019). By responding to such calls for research, the findings of our study highlight the viability of adopting a perspective based on trust theory to understand precautionary security behaviors. Given that security-related situations are rife with uncertainty regarding security threats and grave risks for individuals and organizations, trust theory provides a promising theoretical framework for understanding how employees' trusting beliefs concerning organizational ISec affect their precautionary security behaviors. We note that the protective structures that organizations create to combat security threats could cause employees to trust these structures and thus become complacent regarding security. This unfortunate outcome suggests that trust does not always foster desirable security behaviors. However, this finding represents an important insight for ISec researchers because it can help them understand the conditions under which the precautionary security behaviors of employees become less likely.

Finally, our findings regarding security mindfulness can improve our understanding of the mechanisms that connect trust in organizational ISec with precautionary security behaviors. Our results emphasize the role of mindfulness as a mediator, as proposed by previous IS research (Dernbecher and Beck 2017). However, our results also provide more nuanced insights into this role. Security mindfulness accelerates the positive influence of security commitment on precaution taking and fully mediates the negative influence of security complacency on precaution taking. These insights suggest that mindfulness can not only act as an accelerator of desired beliefs but can also play an important role in mediating undesired beliefs. This finding is important because it emphasizes the mediating role of security mindfulness in both the bright- and dark-side effects of trust. The results also indicate that being mindful of security is an important predictor of precaution-taking behaviors, thereby confirming the view expressed in the literature that precautionary actions require a mindful approach to security, such as in the research indicating that mindful employees are better able to avoid phishing attacks (Jensen et al. 2017).

6.2. Implications for Practice

Encouraging employees to take security precautions is a vital strategy that organizations can use to reduce their vulnerability to various ISec threats. This study has several practical implications regarding the ways in which employees' trust in organizational ISec influences their intention to take security precautions. First, this study highlights that many employees are committed to protecting the organization (mean = 5.81 on a seven-point Likert scale) and are willing to take security precautions (mean = 5.74). The study finds that employees who trust organizational security practices are more committed to protecting the organization and are more willing to take security precautions. To foster trust in organizational security practices and security commitment, ISec managers should establish a trusting security climate via their security training programs to ensure that employees can speak freely about the security problems they face in their work and receive support to resolve those problems if needed. Nurturing trust in this manner may foster hard-to-instill security behaviors such as reporting security breaches, increasing training participation, and overcoming security workarounds and pseudo compliance.

However, this study also alerts managers to the potential adverse consequences of employees' trust in the organization's protective structures. We find that employees' trust in the protective structures established by the organization can backfire, making them complacent regarding security. We observed substantial levels of security complacency among the employees we surveyed (mean = 4.38). Although our study does not dispute the importance of developing protective structures, ISec managers must be aware of the potential adverse effects of these structures. Our study shows that ISec managers can take two types of actions to mitigate these adverse effects. First, as noted above, they can create a trusting security climate to improve employees' trust in organizational security practices because, as our findings show, this type of trust can reduce the complacency of employees. Second, if complacency cannot be avoided or mitigated, implementing zero-trust models can help mitigate the negative consequences of complacent employees because zero-trust models assume that every employee, system, or device can become compromised (Rose et al. 2020). In addition, ISec managers should use security training to emphasize that the organization's protective technological or procedural security countermeasures are insufficient to fend off security threats on their own. Instead, organizational security countermeasures must be complemented by the committed security behaviors of individuals and training that explains how they can take security precautions and why they should be taken (Schuetz et al. 2021).

6.3. Limitations and Directions for Future Research

This study faces certain limitations that indicate avenues for future research. First, because this study uses trust theory as a theoretical lens to examine the ways in which employees' trusting beliefs regarding security in an organizational context relate to their security behaviors, it does not explore or compare alternative theoretical explanations. To this end, one prominent theory that has been advocated by ISec researchers is protection motivation theory (PMT). PMT suggests that individuals' ISec behaviors are driven by their appraisals of threats and the associated coping responses. In line with the findings of PMT researchers that commitment is an important contingent factor of the PMT (Posey et al. 2015), we suggest that researchers should explore the influence of complacency on PMT components. For instance, it would be interesting to investigate whether complacency, as a proxy for employees' heightened confidence in the efficacy of organizational protective structures, affects the relationship between their perceived efficacy of individual protective behaviors and their actual security behavior (Haag et al. 2021).

Second, we collected the data concerning the dependent and independent variables simultaneously, which could have led to the influence of CMB on our data. Although we designed our study carefully to minimize this risk, future research could separate data collection temporally or employ more objective measures of security behaviors (e.g., log data). We see particular value in the possibility of exploring the concept of complacency in the context of security by conducting behavioral experiments that could help validate the empirical insights found by this study. Third, our study uses the online panel provided by Qualtrics to reach study participants from the United States. Because previous research has suggested that cultural effects can influence security behaviors (Chen and Zahedi 2016, Vance et al. 2020), we propose that researchers should investigate our findings in different cultural contexts. Fourth, our study focused on examining precaution taking that is associated with behaviors in which individuals typically engage prior to the occurrence of critical security incidents (e.g., data breaches). It would be fruitful to explore whether critical security incidents shape employees' beliefs regarding security commitment and security complacency and, if they do have such an effect, how long it lasts. Similarly, identifying antecedents and alternative consequences of security complacency would be worthwhile. For example, researchers could investigate whether psychological contract breaches (Zhao et al. 2007) increase complacency beliefs, potentially fueling the problematic consequences of such beliefs. Similarly, future theoretical and empirical research could also examine the influence of security commitment and complacency on security-related outcomes on the opposite side of the spectrum from individual security behaviors, such as noncompliant security behaviors.

Finally, we acknowledge that individuals can attribute trust regarding, for example, the organization, a technology artifact (e.g., antimalware software), or a person (e.g., a security representative) in different ways. There are many forms of trust, such as affective trust, cognitive trust, trust in a specific technology, swift trust, interpersonal trust, distrust, and trust transfer, among others. Although this study focuses on organizational trust, it could be a fruitful avenue for trust researchers to study the bright- and dark-side consequences of different forms of trust in different contexts and with different conditional factors such as culture and industry. Whereas this study considers trust in organizational security practices and trust in organizational protective structures to be an overarching concept that reflects the sociotechnical nature of security in organizations (Dhillon and Backhouse 2001, Dhillon et al. 2021), future research could study and make distinctions related to trust in different entities and contexts in further detail.

7. Conclusion

Motivated by the mixed results reported in the literature concerning the bright- and dark-side effects of trust, this study investigated the bright- and dark-side effects of trust in organizational ISec on precaution taking. By studying both effects within the framework of an integrated theoretical model, we overcome the limitation of focusing on one side of trust while neglecting the other side that is prevalent in related research. The results of this study show that bright-side trust in ISec is associated with a reduction in security complacency and an increase in employees' commitment to and mindfulness regarding security, which encourages employees to take security precautions. We also verified security complacency as a dark-side effect of trust by showing that trust in organizational protective structures reduces employees' security mindfulness. Overall, our findings indicate that the bright-side effects of trust in ISec are more notable than its dark-side effects. Future ISec research can build on the duality of commitment and complacency in the context of ISec to explore the relevance of these factors in other contexts.

Acknowledgments

The authors thank the reviewers, the associate editor, and the senior editor for their helpful comments.

Endnotes

[1] We consider the negative effects of trust to be distinct from distrust, because trust and distrust are distinguishable concepts with their own antecedents and consequences (Dimoka 2010).

[2] Following extant IS research on mindfulness and the original work of Langer (1989), we conceive security mindfulness as state and not as trait (e.g., Dane 2011) because organizations can promote a state of mindfulness (e.g., by training) rather than profoundly changing employees' individual traits (Dernbecher and Beck 2017).

References

Allen NJ, Meyer JP (1990) The measurement and antecedents of affective, continuance and normative commitment to the organization. *J. Occupational Psych.* 63(1):1–18.

Anderson CL, Agarwal R (2010) Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quart.* 34(3):613–643.

Atkinson C (2007) Trust and the psychological contract. *Employee Relations* 29(3):227–246.

Aurigemma S, Leonard L (2015) The influence of employee affective organizational commitment on security policy attitudes and compliance intentions. *J. Inform. Systems Security* 11(3):201–222.

Boss SR, Kirsch LJ, Angermeier I, Shingler RA, Boss RW (2009) If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *Eur. J. Inform. Systems* 18(2):151–164.

Burns AJ (2019) Security organizing: A framework for organizational information security mindfulness. *ACM SIGMIS Database* 50(4):14–27.

Burns AJ, Roberts TL, Posey C, Lowry PB (2019) The adaptive roles of positive and negative emotions in organizational insiders' security-based precaution taking. *Inform. Systems Res.* 30(4):1228–1247.

Burns AJ, Roberts TL, Posey C, Bennett RJ, Courtney JF (2018) Intentions to comply vs. intentions to protect: A VIE theory approach to understanding the influence of insiders' awareness of organizational SETA efforts. *Decision Sci.* 49(6):1187–1228.

Chen Y, Zahedi FM (2016) Individuals' Internet security perceptions and behaviors: Polycontextual contrasts between the United States and China. *MIS Quart.* 40(1):205–222.

Cheung GW, Rensvold RB (2002) Evaluating goodness-of-fit indexes for testing measurement invariance. *Structural Equation Model.* 9(2):233–255.

Chin WW, Thatcher JB, Wright RT, Steel D (2013) Controlling for common method variance in PLS analysis: The measured latent marker variable approach. Abdi H, Chin W, Esposito Vinzi V, Russolillo G, Trinchera L, eds. *New Perspectives in Partial Least Squares and Related Methods* (Springer, New York), 231–239.

Choi SB, Tran TBH, Park BI (2015) Inclusive leadership and work engagement: Mediating roles of affective organizational commitment and creativity. *Soc. Behav. Personality* 43(6):931–943.

Chowdhury NH, Adam MT, Teubner T (2020) Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. *Comput. Security* 97:101963.

Christensen-Salem A, Walumbwa FO, Babalola MT, Guo L, Misati E (2021) A multilevel analysis of the relationship between ethical leadership and ostracism: The roles of relational climate, employee mindfulness, and work unit structure. *J. Bus. Ethics* 171(3):619–638.

Colquitt JA, Scott BA, LePine JA (2007) Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance. *J. Appl. Psych.* 92(4):909–927.

Coyle-Shapiro JA-M, Kessler I (2002) Exploring reciprocity through the lens of the psychological contract: Employee and employer perspectives. *Eur. J. Work Organ. Psych.* 11(1):69–86.

Cram WA, D'Arcy J, Proudfoot JG (2019) Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quart.* 43(2):525–554.

Curcuruto M, Griffin MA (2016) Safety proactivity in the workplace: The initiative to improve individual, team, and organizational safety. Parker SK, Bindl UK, eds. *Proactivity at Work: Making Things Happen in Organizations*, Organization and Management Series (Routledge, New York), 221–238.

Curcuruto M, Parker SK, Griffin MA (2019) Proactivity toward workplace safety improvement: An investigation of its motivational drivers and organizational outcomes. *Eur. J. Work Organ. Psych.* 28(2):221–238.

Dane E (2011) Paying attention to mindfulness and its effects on task performance in the workplace. *J. Management* 37(4):997–1018.

D'Arcy J, Hovav A, Galletta D (2009) User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Inform. Systems Res.* 20(1):79–98.

Davis J, Agrawal D, Guo X (2023) Enhancing users' security engagement through cultivating commitment: The role of psychological needs fulfilment. *Eur. J. Inform. Systems* 32(2):195–206.

Dernbecher S, Beck R (2017) The concept of mindfulness in information systems research: A multi-dimensional analysis. *Eur. J. Inform. Systems* 26(2):121–142.

Dhillon G, Backhouse J (2001) Current directions in IS security research: Toward socio-organizational perspectives. *Inform. Systems J.* 11(2):127–153.

Dhillon G, Smith K, Dissanayaka I (2021) Information systems security research agenda: Exploring the gap between research and practice. *J. Strategic Inform. Systems* 30(4):101693.

Dillon RL, Tinsley CH (2008) How near-misses influence decision making under risk: A missed opportunity for learning. *Management Sci.* 54(8):1425–1440.

Dimoka A (2010) What does the brain tell us about trust and distrust? Evidence from a functional neuroimaging study. *MIS Quart.* 34(2):373–396.

Dinev T, Hu Q (2007) The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *J. Assoc. Inform. Systems* 8(7):387–408.

Dirks KT, Ferrin DL (2001) The role of trust in organizational settings. *Organ. Sci.* 12(4):450–467.

Dirks KT, Ferrin DL (2002) Trust in leadership: Meta-analytic findings and implications for research and practice. *J. Appl. Psych.* 87(4):611–628.

Faul F, Erdfelder E, Buchner A, Lang AG (2009) Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behav. Res. Methods* 41(4):1149–1160.

Fornell C, Larcker DF (1981) Evaluating structural equation models with unobservable variables and measurement error. *J. Marketing Res.* 18(1):39–50.

Fulmer CA, Gelfand MJ (2012) At what level (and in whom) we trust. *J. Management* 38(4):1167–1230.

Gargiulo M, Ertug G (2006) The dark side of trust. Bachmann R, Zaheer A, eds. *Handbook of Trust Research* (Edward Elgar Publishing, Cheltenham, UK), 165–186.

Gefen D, Benbasat I, Pavlou P (2008) A research agenda for trust in online environments. *J. Management Inform. Systems* 24(4):275–286.

Gefen D, Karahanna E, Straub DW (2003) Trust and TAM in online shopping: An integrated model. *MIS Quart.* 27(1):51–90.

Gefen D, Rigdon EE, Straub DW (2011) Editor's comments: An update and extension to SEM guidelines for administrative and social science research. *MIS Quart.* 35(2):iii–xiv.

Gilbert JA, Tang TLP (1998) An examination of organizational trust antecedents. *Public Personnel Management* 27(3):321–338.

Gouldner AW (1960) The norm of reciprocity: A preliminary statement. *Amer. Sociol. Rev.* 25(2):161.

Guan B, Hsu C (2020) The role of abusive supervision and organizational commitment on employees' information security policy noncompliance intention. *Internet Res.* 30(5):1383–1405.

Guo KH, Yuan Y, Archer NP, Connelly CE (2011) Understanding nonmalicious security violations in the workplace: A composite behavior model. *J. Management Inform. Systems* 28(2):203–236.

Haag S, Siponen M, Liu F (2021) Protection motivation theory in information systems security research. *ACM SIGMIS Database* 52(2):25–67.

Henseler J, Ringle CM, Sarstedt M (2015) A new criterion for assessing discriminant validity in variance-based structural equation modeling. *J. Acad. Marketing Sci.* 43(1):115–135.

Herath T, Rao HR (2009a) Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems* 47(2):154–165.

Herath T, Rao HR (2009b) Protection motivation and deterrence: A framework for security policy compliance in organisations. *Eur. J. Inform. Systems* 18(2):106–125.

Herath TC, Herath HSB, D'Arcy J (2020) Organizational adoption of information security solutions. *ACM SIGMIS Database* 51(2):12–35.

Hong W, Chan KY, Thong JYL, Chasalow LC, Dhillon G (2014) A framework and guidelines for context-specific theorizing in information systems research. *Inform. Systems Res.* 25(1):111–136.

Hsu JS, Shih SP, Hung YW, Lowry PB (2015) The role of extra-role behaviors and social controls in information security policy effectiveness. *Inform. Systems Res.* 26(2):282–300.

Hu L, Bentler PM (1999) Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria vs. new alternatives. *Structural Equation Model.* 6(1):1–55.

Ifinedo P (2014) Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Inform. Management* 51(1):69–79.

Jaeger L, Eckhardt A (2021) Eyes wide open: The role of situational information security awareness for security-related behaviour. *Inform. Systems J.* 31(3):429–472.

Jafri MH (2010) Organizational commitment and employee's innovative behavior. *J. Management Res.* 10(1):62–68.

Jenkins JL, Anderson BB, Vance A, Kirwan CB, Eargle D (2016) More harm than good? How messages that interrupt can make us vulnerable. *Inform. Systems Res.* 27(4):880–896.

Jensen ML, Dinger M, Wright RT, Thatcher JB (2017) Training to mitigate phishing attacks using mindfulness techniques. *J. Management Inform. Systems* 34(2):597–626.

Jeon S, Hovav A, Han J, Alter S (2018) Rethinking the prevailing security paradigm. *ACM SIGMIS Database* 49(3):54–77.

Karjalainen M, Sarker S, Siponen M (2019) Toward a theory of information systems security behaviors of organizational employees: A dialectical process perspective. *Inform. Systems Res.* 30(2):687–704.

Khuntia J, Kathuria A, Andrade-Rojas MG, Saldanha TJV, Celly N (2021) How foreign and domestic firms differ in leveraging IT-enabled supply chain information integration in BOP markets: The role of supplier and client business collaboration. *J. Assoc. Inform. Systems* 22(3):695–738.

Kline RB (2016) *Principles and Practice of Structural Equation Modeling*, 4th ed. (Guilford Press, New York).

Kock N, Lynn G (2012) Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations. *J. Assoc. Inform. Systems* 13(7):546–580.

Komiak SYX, Benbasat I (2006) The effects of personalization and familiarity on trust and adoption of recommendation agents. *MIS Quart.* 30(4):941–960.

Krishnan R, Martin X, Noorderhaven NG (2006) When does trust matter to alliance performance? *Acad. Management J.* 49(5):894–917.

Landis JR, Koch GG (1977) The measurement of observer agreement for categorical data. *Biometrics* 33(1):159.

Langer EJ (1989) Minding matters: The consequences of mindlessness–mindfulness. *Adv. Experiment. Soc. Psych.* 22:137–173.

Langer EJ (2014) *Mindfulness*, 25th anniversary ed. (Da Capo Press, Philadelphia).

Langfred CW (2004) Too much of a good thing? Negative effects of high trust and individual autonomy in self-managing teams. *Acad. Management J.* 47(3):385–399.

Lewis JD, Weigert A (1985) Trust as a social reality. *Soc. Forces* 63(4):967–985.

Liang H, Xue Y (2009) Avoidance of information technology threats: A theoretical perspective. *MIS Quart.* 33(1):71–90.

Liang H, Xue Y, Pinsonneault A, Wu Y (2019) What users do besides problem-focused coping when facing IT security threats: An emotion-focused coping perspective. *MIS Quart.* 43(2):373–394.

Lindell MK, Whitney DJ (2001) Accounting for common method variance in cross-sectional research designs. *J. Appl. Psych.* 86(1):114–121.

Lins S, Becker JM, Lyytinen K, Sunyaev A (2023) A design theory for certification presentations. *SIGMIS Database* 54(3):75–118.

Lins S, Kromat T, Löbbers J, Benlian A, Sunyaev A (2022) Why don't you join in? A typology of information system certification adopters. *Decision Sci.* 53(3):452–485.

Liu C, Wang N, Liang H (2020) Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *Internat. J. Inform. Management* 54:102152.

Loch KD, Carr HH, Warkentin M (1992) Threats to information systems: Today's reality, yesterday's understanding. *MIS Quart.* 16(2):173–186.

Lowry PB, D'Arcy J, Hammer B, Moody GD (2016) 'Cargo cult' science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels. *J. Strategic Inform. Systems* 25(3):232–240.

Lowry PB, Moody GD, Galletta DF, Vance A (2013) The drivers in the use of online whistle-blowing reporting systems. *J. Management Inform. Systems* 30(1):153–190.

Lowry PB, Posey C, Bennett RBJ, Roberts TL (2015) Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Inform. Systems J.* 25(3):193–273.

MacKinnon DP, Lockwood CM, Williams J (2004) Confidence limits for the indirect effect: Distribution of the product and resampling methods. *Multivariate Behav. Res.* 39(1):99–128.

Macneil IR (1985) Relational contract: What we do and do not know. *Wisconsin Law Rev.* 4:483–525.

Maier C, Laumer S, Wirth J, Weitzel T (2019) Technostress and the hierarchical levels of personality: A two-wave study with multiple data samples. *Eur. J. Inform. Systems* 28(5):496–522.

Markus ML (2017) Datification, organizational strategy, and IS research: What's the score? *J. Strategic Inform. Systems* 26(3):233–241.

Martin SR, Lee JJ, Parmar BL (2021) Social distance, trust and getting "hooked": A phishing expedition. *Organ. Behav. Human Decision Processes* 166:39–48.

Mayer RC, Davis JH, Schoorman FD (1995) An integrative model of organizational trust. *Acad. Management Rev.* 20(3):709–734.

McAllister DJ (1997) The second face of trust: Reflections on the dark side of interpersonal trust in organizations. Lewicki RJ, Bies RJ, Sheppard BH, eds. *Research on Negotiation in Organizations* (JAI Press, Bingley, UK), 87–111.

McKnight DH, Choudhury V, Kacmar C (2002) Developing and validating trust measures for e-commerce: An integrative typology. *Inform. Systems Res.* 13(3):334–359.

McKnight DH, Carter M, Thatcher JB, Clay PF (2011) Trust in a specific technology: An investigation of its components and measures. *ACM Trans. Management Inform. Systems* 2(2):1–25.

Merritt SM, Ako-Brew A, Bryant WJ, Staley A, McKenna M, Leone A, Shirase L (2019) Automation-induced complacency potential: Development and validation of a new scale. *Front. Psych.* 10:1–13.

Meyer JP, Allen NJ (1991) A three-component conceptualization of organizational commitment. *Human Resource Management Rev.* 1(1):61–89.

Meyer JP, Allen NJ (1997) *Commitment in the Workplace: Theory, Research, and Application* (SAGE Publications, Inc, Thousand Oaks, CA).

Mitnick KD (2003) *The Art of Deception: Controlling the Human Element of Security* (Wiley Publishing, Indianapolis).

Möllering G, Sydow J (2019) Trust trap? Self-reinforcing processes in the constitution of inter-organizational trust. Sasaki M, ed. *Trust in Contemporary Society* (Brill Academic Publishers, Boston), 141–160.

Moore GC, Benbasat I (1991) Development of an instrument to measure the perceptions of adopting an information technology innovation. *Inform. Systems Res.* 2(3):192–222.

Mylonas A, Kastania A, Gritzalis D (2013) Delegate the smartphone user? Security awareness in smartphone platforms. *Comput. Security* 34:47–66.

Nguyen C, Jensen ML, Durcikova A, Wright RT (2021) A comparison of features in a crowdsourced phishing warning system. *Inform. Systems J.* 31(3):473–513.

Nunnally JC (1978) *Psychometric Theory*, 2nd ed. (McGraw-Hill, New York).

Nwankpa JK, Datta PM (2023) Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers. *Comput. Security* 130:103266.

Nwankpa JK, Roumani Y (2014) The influence of organizational trust and organizational mindfulness on ERP systems usage. *Comm. Assoc. Inform. Systems* 34:1469–1492.

Parasuraman R, Manzey DH (2010) Complacency and bias in human use of automation: An attentional integration. *Human Factors* 52(3): 381–410.

Parasuraman R, Molloy R, Singh IL (1993) Performance consequences of automation-induced "complacency." *Internat. J. Aviation Psych.* 3(1):1–23.

Parker SK, Collins CG (2010) Taking stock: Integrating and differentiating multiple proactive behaviors. *J. Management* 36(3):633–662.

Parker SK, Wu CH (2014) Leading for proactivity: How leaders cultivate staff who make things happen. Day DV, ed. *The Oxford Handbook of Leadership and Organizations* (Oxford University Press, New York), 380–403.

Pavlou PA, Liang H, Xue Y (2007) Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quart.* 31(1):105–136.

Pfleeger SL, Sasse MA, Furnham A (2014) From weakest link to security hero: Transforming staff security behavior. *J. Homeland Security Emergency Management* 11(4):489–510.

Pienta D, Tams S, Thatcher JB (2020) Can trust be trusted in cybersecurity? *Proc. 53rd Hawaii Internat. Conf. System Sci.*, 4264–4273.

Podsakoff PM, MacKenzie SB, Lee JY, Podsakoff NP (2003) Common method biases in behavioral research: A critical review of the literature and recommended remedies. *J. Appl. Psych.* 88(5):879–903.

Posey C, Bennett RJ, Roberts TL (2011a) Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Comput. Security* 30(6–7):486–497.

Posey C, Roberts TL, Lowry PB (2015) The impact of organizational commitment on insiders' motivation to protect organizational information assets. *J. Management Inform. Systems* 32(4):179–214.

Posey C, Bennett RJ, Roberts TL, Lowry PB (2011b) When computer monitoring backfires: Privacy invasions and organizational injustice as precursors to computer abuse. *J. Inform. System Security* 7(1): 24–47.

Posey C, Roberts TL, Lowry PB, Hightower RT (2014) Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Inform. Management* 51(5):551–567.

Posey C, Roberts TL, Lowry PB, Bennett RJ, Courtney JF (2013) Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quart.* 37(4):1189–1210.

Robinson SL (1996) Trust and breach of the psychological contract. *Admin. Sci. Quart.* 41(4):574–599.

Rose S, Mitchell S, Connelly S (2020) Zero trust architecture. Accessed May 23, 2022, https://doi.org/10.6028/NIST.SP.800-207.

Rousseau DM, Sitkin SB, Burt RS, Camerer C (1998) Not so different after all: A cross-discipline view of trust. *Acad. Management Rev.* 23(3):393–404.

Sadok M, Alter S, Bednar P (2020) It is not my job: Exploring the disconnect between corporate security policies and actual security practices in SMEs. *Inform. Comput. Security* 28(3):467–483.

Sarkar S, Vance A, Ramesh B, Demestihas M, Wu DT (2020) The influence of professional subculture on information security policy violations: A field study in a healthcare context. *Inform. Systems Res.* 31(4):1240–1259.

Schaufeli WB, Salanova M, González-romá V, Bakker AB (2002) The measurement of engagement and burnout: A two sample confirmatory factor analytic approach. *J Happiness Stud.* 3(1):71–92.

Schoorman FD, Mayer RC, Davis JH (2007) An integrative model of organizational trust: Past, present, and future. *Acad. Management Rev.* 32(2):344–354.

Schuetz SW, Lowry PB, Pienta D, Thatcher JB (2021) Improving the design of information security messages by leveraging the effects of temporal distance and argument nature. *J. Assoc. Inform. Systems* 22(5):1376–1428.

Singh IL, Molloy R, Parasuraman R (1993) Automation-induced "complacency": Development of the complacency-potential rating scale. *Internat. J. Aviation Psych.* 3(2):111–122.

Siponen M, Puhakainen P, Vance A (2020) Can individuals' neutralization techniques be overcome? A field experiment on password policy. *Comput. Security* 88:101617.

Skinner D, Dietz G, Weibel A (2014) The dark side of trust: When trust becomes a "poisoned chalice." *Organization* 21(2):206–224.

Spector PE, Brannick MT (2011) Methodological urban legends: The misuse of statistical control variables. *Organ. Res. Methods* 14(2):287–305.

Stafford TF (2022) Platform-dependent computer security complacency: The unrecognized insider threat. *IEEE Trans. Engrg. Management* 69(6):3814–3825.

Straub DW (1989) Validating instruments in MIS research. *MIS Quart.* 13(2):147–169.

Straub DW (1990) Effective IS security: An empirical study. *Inform. Systems Res.* 1(3):255–276.

Sutcliffe KM, Vogus TJ, Dane E (2016) Mindfulness in organizations: A cross-level review. *Annual Rev. Organ. Psych. Organ. Behav.* 3(1):55–81.

Swanson EB, Ramiller NC (2004) Innovating mindfully with information technology. *MIS Quart.* 28(4):553–583.

Tan HH, Lim AKH (2009) Trust in coworkers and trust in organizations. *J. Psych.* 143(1):45–66.

Tessian (2021) Back to work security behaviors report. Accessed June 24, 2021, https://www.tessian.com/resources/back-to-work-cybersecurity-behaviors-report/.

Thatcher JB, Wright RT, Sun H, Zagenczyk TJ, Klein R (2018) Mindfulness in information technology use: Definitions, distinctions, and a new measure. *MIS Quart.* 42(3):831–847.

Vance A, Siponen MT, Straub DW (2020) Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. *Inform. Management* 57(4):103212.

Vogus TJ, Sutcliffe KM (2012) Organizational mindfulness and mindful organizing: A reconciliation and path forward. *Acad. Management Learn. Educ.* 11(4):722–735.

Wang J, Li Y, Rao HR (2016) Overconfidence in phishing email detection. *J. Assoc. Inform. Systems* 17(11):759–783.

Warkentin M, Willison R (2009) Behavioral and policy issues in information systems security: The insider threat. *Eur. J. Inform. Systems* 18(2):101–105.

Williams LJ, Hartman N, Cavazotte F (2010) Method variance and marker variables: A review and comprehensive CFA marker technique. *Organ. Res. Methods* 13(3):477–514.

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

Wong YT, Ngo HY, Wong CS (2002) Affective organizational commitment of workers in chinese joint ventures. *J. Management Psych.* 17(7):580–598.

Wood SL, Lynch JG (2002) Prior knowledge and complacency in new product learning. *J. Consumer Res.* 29(3):416–426.

Workman M (2008) Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *J. Amer. Soc. Inform. Sci. Tech.* 59(4):662–674.

Wright RT, Campbell DE, Thatcher JB, Roberts N (2012) Operationalizing multidimensional constructs in structural equation modeling: Recommendations for IS research. *Comm. Assoc. Inform. Systems* 30:367–412.

Xu F, Hsu C, Luo X, Warkentin M (2022) Reactions to abusive supervision: Neutralization and IS misuse. *J. Comput. Inform. Systems* 62(3):632–641.

Yazdanmehr A, Wang J (2021) Can peers help reduce violations of information security policies? The role of peer monitoring. *Eur. J. Inform. Systems* 32(3):508–528.

Zhao H, Wayne SJ, Glibkowski BC, Bravo J (2007) The impact of psychological contract breach on work-related outcomes: A meta-analysis. *Personnel Psych.* 60(3):647–680.

Zhao X, Lynch JG, Chen Q (2010) Reconsidering Baron and Kenny: Myths and truths about mediation analysis. *J. Consumer Res.* 37(2):197–206.

Zucker LG (1983) Organizations as institutions. Bacharach S, ed. *Research in the Sociology of Organizations* (JAI Press, Greenwich, CT), 1–47.