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

INFORMATION SYSTEMS RESEARCH
Articles in Advance, pp. 1–13
ISSN 1047-7047 (print), ISSN 1526-5536 (online)

Promoting Security Behaviors in Remote Work Environments: Personal Values Shaping Information Security Policy Compliance

Carlos I. Torres,[a,*] **Robert E. Crossler**[b]

[a] ISBA Department, Hankamer School of Business, Baylor University, Waco, Texas 76798; [b] MISE Department, Carson College of Business, Washington State University, Pullman, Washington 99164

*Corresponding author

Contact: carlos_torres@baylor.edu, https://orcid.org/0000-0002-9819-467X (CIT); rob.crossler@wsu.edu, https://orcid.org/0000-0002-8179-9138 (REC)

Received: November 4, 2021
Revised: December 21, 2022; February 21, 2024
Accepted: May 23, 2024
Published Online in Articles in Advance: July 1, 2024

https://doi.org/10.1287/isre.2021.0563

Abstract. Cybersecurity threats and information security policy (ISP) compliance are critical concerns for organizations. The recent trend of working from home has made individual characteristics more relevant in fostering ISP compliance. Whereas extant research has theorized and offered alternatives to induce ISP compliance, most studies have failed to consider the differences between onsite and remote workers to motivate compliance with ISPs and have instead focused on standard interventions without considering personal characteristics. One of the few models including factors related to individuals' characteristics is the unified model of information security policy compliance (UMISPC). This paper extends the UMISPC by drawing on Schwartz's universal theory of personal values. We propose the values construct as a robust representation of an individual's motivations to comply with an ISP. We confirm that personal values are significant predictors of compliance with ISPs. Furthermore, a comparison between onsite and remote workers suggests that personal values are more relevant in remote work settings. Our findings shed light on the values and individual characteristics that are important motivators for ISP compliance and how they differ for onsite and remote workers. Our results suggest that people's personal motivations should be considered in promoting organizations' ISPs and that organizations' interventions should be tailored by understanding what values motivate or hinder ISP compliance.

History: Manju Ahuja, Senior Editor; Debabrata Dey, Associate Editor.
Supplemental Material: The online appendix is available at https://doi.org/10.1287/isre.2021.0563.

Keywords: UMISPC • personal values • ISP compliance • values • remote work • hybrid work

Introduction

Cybersecurity remains the most pressing issue for organizations' chief information officers (Johnson et al. 2023), with global data breach costs growing from $3.86 million per incident in 2018 to $4.45 million in 2023, with even greater financial losses when the data breach involves remote access (IBM 2023). Even considering these increased data breach costs, remote work will remain the new norm for organizations of all sizes. The effects of the COVID-19 pandemic have been substantial, with knowledge workers leaving urban areas and relying more on remote or hybrid work and office attendance in 2023 stabilizing at 30% below pre-pandemic levels (McKinsey 2023). Companies have been challenged to adapt their cybersecurity postures to prevent different sets of cyberthreats from targeting remote employees (Rahamti 2023). Unfortunately, despite preventive efforts in both remote and onsite environments, employees' lack of commitment to cybersecurity continues to be the main challenge for information security (infosec) teams, as evidenced by 74% of data breaches involving human elements, such as errors, misuse, or lack of compliance with information security policies (ISPs) (Verizon 2023).

With people working more from home, organizations need to shift their infosec approach to being more individual oriented (Nyarko and Fong 2023, Whitty et al. 2024). Most top management teams are pushing for new strategies and initiatives when designing and implementing ISPs for remote environments (Rahamti 2023). This situation makes studying different alternatives that take individual characteristics, such as personal values, and their influence on ISP compliance into consideration an open field of research in the broader cybersecurity arena. Furthermore, considering that humans continue to be the weakest link in infosec (Perez 2022,

Verizon 2023), individual characteristics like values and personality are becoming more relevant in fostering ISP compliance in environments with fewer infosec controls, such as remote work environments.

Scholars have theorized about the potential reasons why employees behave in a manner contrary to ISPs to explain and prevent cyber risks (see, e.g., Siponen and Vance 2010, Boss et al. 2015, Greulich et al. 2024). These efforts to explain and understand ISP compliance have provided insights into such compliance in the workplace, suggesting general interventions targeting widespread security issues. However, with cyberthreats increasingly targeting individuals working from home, organizations are struggling to implement policies or interventions to prevent cybersecurity events (Rahamti 2023). Furthermore, the current hybrid work trend (McKinsey 2023), fueled by the expanding ease and popularity of working from home, calls for a review and update of all enforcement procedures related to ISP compliance (Nyarko and Fong 2023).

Research conducted after the COVID-19 pandemic, when remote work has noticeably increased, has shown that despite organizations' compliance frameworks and infosec practices, ISP compliance levels are low in remote environments (Nyarko and Fong 2023, Whitty et al. 2024). As a result, research has called for scholars and practitioners to consider personal factors when studying infosec interventions "instead of a 'one-size-fits-all approach'" (Whitty et al. 2024, p. 1). However, differences in motivations to perform secure behaviors between onsite and remote workers have remained relatively unexplored in the infosec literature, with the above-mentioned examples relating only to remote work. The new hybrid work trend has opened research opportunities to explore how ISP compliance differs in remote environments (vis-à-vis in onsite environments) and how individuals' characteristics (e.g., personality, values), which have become more relevant in developing new policies, can influence ISP compliance in these environments.

Our research contributes to the infosec literature by exploring differences in ISP compliance in remote work environments (vis-à-vis in onsite environments). This paper focuses on personal values as a unique aspect related to security interventions that can explain differences in security behaviors in various work environments. Personal values are an intrinsic part of individuals, generally defined as a broad set of desirable goals motivating people's actions as guiding principles in their lives. These values also reflect individual characteristics that hold higher explanatory potential in relation to behaviors because people act according to what their beliefs indicate (Sagiv and Roccas 2021).

The unified model for information security policy compliance (UMISPC) (Moody et al. 2018) is one of the first infosec theories we are aware of that includes a values construct as a direct predictor of compliance with ISPs. However, there is no clear conceptualization of the values construct in the UMISPC, generating an opportunity for our research to extend this model by introducing a proper theorization of the personal values that influence ISP compliance.

In this project, we introduce Schwartz's (1992) theory of personal values to explain ISP compliance behaviors and differences in infosec behaviors between onsite and remote workers. The theory of personal values is an excellent fit to explain general values-behaviors relationships because it covers the full spectrum of values, their application as direct predictors of behaviors, and the possibility of change with interventions. Despite its applicability, this theory has scarcely been used in information systems research (Tams et al. 2020, Elo et al. 2022). We contend that personal values (Schwartz 1992) play a significant role in individuals' ISP compliance intentions. Furthermore, we suggest the critical role of personal values in ISP compliance in less supervised environments, such as remote work environments. In doing so, we address the following research questions: *How do personal values explain individuals' different protective behavioral intentions for ISP compliance? How do remote and onsite workers differ in their motivations to comply with ISPs?*

Our research supports the fact that in the new hybrid work environments, important differences in ISP compliance are arising for organizations, particularly with remote workers. We reveal that values are significant predictors of behavioral intentions to comply with ISPs. We also show that the significance of those intentions varies and becomes more relevant in remote work settings. Our research suggests that personal values are one of the factors that need to be taken into consideration in ISP design, enforcement, training, and communication oriented toward employees working from home.

Literature Review

Personal Values

The theory of personal values offers a framework for investigating values from either a collective or a personal standpoint (Schwartz 1994). The types of personal values defined by Schwartz are unique and apply to all humans regardless of the level of study (Rohan 2000). Personal values are universally acknowledged as trans-situational objectives that fix a person's positions and actions in life (Cisłak et al. 2022). Schwartz organized human values as a circular continuum (Schwartz 1992, Schwartz et al. 2012) to

reflect the values-related congruence or conflict people encounter on a daily basis (Schwartz 1992, 1994).

Despite the general use of the term values to refer to attitudes or beliefs (see, e.g., Cram et al. 2019), the theory of personal values is comprehensive and posits that all humans have a value system comprising a specific number of value types. Still, each person places relative priority on each type (Rohan 2000). Schwartz (1992) emphasized that there will always be conflicting differences in prioritizing opposite values along a continuum.

Schwartz's theory enables differentiation between different levels of abstraction within a motivational hierarchy. The 19 first-order values are more detailed but can be organized into a set of four more general value types (second-order values). The four second-order value types align with motivational organizing principles that can be considered antagonistic (e.g., personal-oriented or group-oriented focus). The motivational organizing principles allow researchers to study fundamental human values for different scholarly purposes (Cisłak et al. 2022). Values or orientations found on opposing sides of the continuum reflect conflicting motivations. As a result, actions, choices, or behaviors that support one value are likely to undermine the value they are meant to counter (Cisłak et al. 2022). Thus, behaviors, opinions, and decisions motivated by one value tend to simultaneously undermine actions supported by values that are located on the opposite side of the continuum (Cisłak et al. 2022).

A summary of the 19 first-order values with the motivational goals that define them (Sagiv and Schwartz 2022) is presented in Table 1. The values literature summarizes the values construct as multidimensional, which is comprised of a two-dimensional structure (Rohan 2000, Schwartz et al. 2017, Sagiv and Schwartz 2022). The values construct can be parsimoniously defined as comprising "four higher-order value types that form two basic, bipolar, conceptual dimensions" (Schwartz 1992, p. 43). The higher-order (i.e., second-order) constructs are measured at a higher level of abstraction (Sarstedt et al. 2019, Ringle et al. 2022). In the case of the values construct, these two bipolar dimensions are (1) openness to change versus conservation and (2) self-enhancement versus self-transcendence.

The first bipolar dimension is openness to change versus conservation. Basic values, such as stimulation and self-direction, are included in openness to change, whereas conformity, tradition, and security are included in conservation. Novelty and change are at one end of this dimension; on the other end is stability (Cisłak et al. 2022).

The second dimension is self-transcendence versus self-enhancement. Self-enhancement includes values like power and achievement, whereas universalism, benevolence, and altruism form the self-transcendence second-order construct. This second dimension, consequently, encompasses self-interest and sentiments of social superiority on one end and helping others and going above and beyond self-interest on the other end (Cisłak et al. 2022).

Unified Model for Information Security Policy Compliance

In an effort to synthesize the different theories on ISP compliance, Moody et al. (2018) conceptualized the UMISPC by extracting elements from the 11 leading

Table 1. Summary of the Four Higher-Order Values, Basic Values, and Motivational Goals

Second-order construct	First-order construct	Motivational goals (definition)
Openness to change	Self-direction: thought	Freedom to cultivate one's own ideas and abilities
	Self-direction: action	Freedom to determine one's own actions
	Stimulation	Excitement, novelty, and challenge in life
	Hedonism	Pleasure and sensuous gratification for oneself
Self-enhancement	Achievement	Personal success through demonstrating competence according to social standards
	Power: dominance	Power through exercising control over people
	Power: resources	Power through control of material and social resources
	Face	Maintaining one's public image and avoiding humiliation
Conservation	Security: personal	Safety in one's immediate environment
	Security: societal	Safety and stability in the wider society
	Conformity: rules	Conformity with rules, laws, and formal obligations
	Conformity: interpersonal	Avoidance of upsetting or harming other people
	Tradition	Maintaining and preserving cultural family or religious traditions
	Humility	Recognizing one's insignificance in the larger scheme of things
Self-transcendence	Benevolence: dependability	Being a reliable and trustworthy member of the ingroup
	Benevolence: caring	Commitment to the welfare of ingroup members
	Universalism: concern	Commitment to equality, justice, and protection for all people
	Universalism: nature	Preservation of the natural environment
	Universalism: tolerance	Acceptance and understanding of those who are different from oneself

Note. Adapted from Sagiv and Schwartz (2022).

theories in the ISP compliance literature. The authors combined several constructs into more general ones to reduce the model's complexity. Moody et al. (2018) included different traditionally analyzed constructs from the infosec literature in their UMISPC model as the basis for uncovering the best data-driven explanation of compliance.

All of the UMISPC constructs have been traditionally linked to intentions to comply with security policies, with the values construct being the only exception. These relationships are illustrated in Figure 1 as the unmodified UMISPC hypotheses. Threat is the perceived seriousness or magnitude of a risk associated with a given behavior. Fear is a negative emotion elicited by the perceived threat, resulting in increased arousal. Habits are automatic behaviors that are performed without paying attention. Neutralization is related to behaviors that offer a way to render norms inoperative while justifying them, and reactance is an adverse reaction toward the suggested secure behaviors (Moody et al. 2018). The infosec literature has commonly included fear as a predictor of intention, which is also produced as an outcome of threat (Boss et al. 2015). Based on Siponen and Vance (2010) adaptation of the theory of neutralization, Moody et al. (2018) included reactance as a route for denying the possible infosec problem as an alternative way for individuals to cope with fear, and they considered that it may have different antecedents, such as neutralization. They also added a "role values" construct that was not in any of the original tested models.

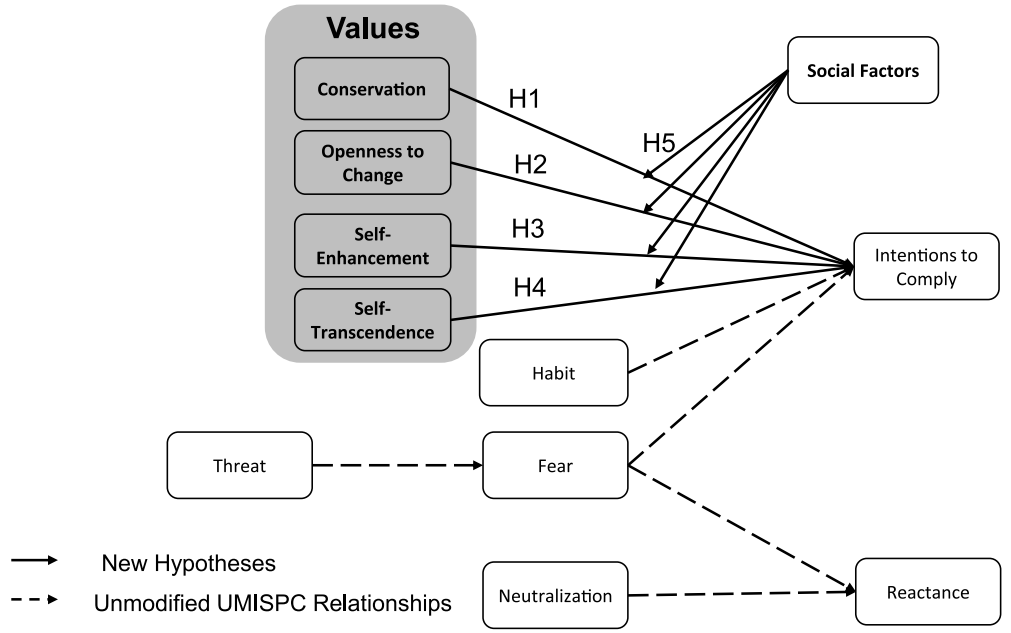
Moody et al. (2018) found support for the proposed dual pathway (intention and reactance) as well as for the habit, fear, and role values being predictors of intentions to comply, whereas neutralization and fear were found to predict reactance. As per the results of their study, they proposed the final refined version of their UMISPC model, which is the basis for our conceptualization effort.

Moody et al.'s Factor 1, called "role values," had the most considerable impact on intentions to comply. How Factor 1 represents role values was not fully explained in the article, and the literature does not provide further support for how this construct influences individuals' intentions to comply with ISPs.

Hypothesis Formulation and Research Model

Utilizing Schwartz's (1992) theory of personal values in our project, we modified the UMISPC, resulting in our research model and hypotheses. Considering that the role values construct was not initially part of the analyzed and defined constructs in the UMISPC, we speculated that the Factor 1 construct partially represents the values construct. Figure 1 summarizes our theoretical model, including the values construct defined by Schwartz, thus presenting a modified version of the UMISPC. The model draws on the theory of personal values (Schwartz 1992) to identify whether and what type of values are significant predictors of intentions to comply with ISPs. Thus, we

Figure 1. Proposed Modified UMISPC Research Model



replicated the other UMISPC relationships without adapting any hypotheses.

Feldman et al. (2015) studied motivators and inhibitors of rule-breaking. Their study was motivated by reactions to ethical scandals in business that associated unethical behaviors with "falling moral standards caused by lack of values" (Feldman et al. 2015, p. 69). Based on the theory of personal values (Schwartz 1992), they explained how personal values are associated with rule-breaking behaviors and how some second-order values constructs are better predictors of rule-breaking behaviors than others. Accordingly, we introduced the second-order values constructs in our model and hypotheses as an innovative concept rarely explored in IS research.

The theory of personal values considers that values work as a system rather than as disconnected singular values (Schwartz 1992, Sagiv and Schwartz 2022), a conceptualization that has found consistent empirical support (see, e.g., Cieciuch et al. 2014 and Schwartz et al. 2017). Indeed, "Values are considered central to the self, stable, enduring, universal, and trans-situational" (Feldman et al. 2015, p. 70). In the theory of personal values, values are grouped into categories with universal meaning on a circular model with a structure of relationships (see, e.g., Schwartz et al. 2012 and Schwartz et al. 2017). As Feldman et al. (2015, p. 71) explained,

> The circumplex structure of personal values and the inherent conflict between values at the opposite ends of a dimension means that the promotion of certain value-expressive behaviors in a certain direction comes at the expense of value-expressive behaviors in the other direction (Bardi and Schwartz 2003, Frimer and Walker 2009). Therefore, the tension between conflicting interpretations of value-related behaviors is an integral part of the values circumplex structure.

The two bipolar dimensions can parsimoniously define the complex personal values system. Still, any value-motivated behavior requires a trade-off between opposite values. When evidence suggests that one of the bipolar dimensions would trigger a positive or negative association with a behavior, it must be assumed that the action violates values on the other side of the bipolar dimension, triggering the opposite association on the other side (Feldman et al. 2015, Schwartz et al. 2017).

Conservation includes values related to upholding traditions, maintaining security, ensuring conformity, motivating self-discipline, sustaining the status quo, and striving to maintain long-term relationships in order to either conform to societal rules and norms or to avoid change (Sagiv and Schwartz 2022). Conservation values negatively correlate with the tendency to take risks (Weinstein et al. 2020). However, even in the presence of conservation values, when a person demonstrates respect for tradition and authority, they may break the rules if those rules are against such values (Sagiv and Schwartz 2022). Considering the context of ISP compliance, conservation values likely significantly affect infosec behaviors. However, the size and direction of this relationship can vary, depending on context and the specific ISP under evaluation. Thus, we propose that conservation values have a direct effect on people's compliance with ISPs.

Hypothesis 1. *Conservation values influence compliance with ISPs.*

Openness to change prioritizes values in a way that motivates individuals to pursue their interests (whether economic, intellectual, or emotional), sometimes in riskier directions than other people would pursue (Schwartz et al. 2017). Feldman et al. (2015) concluded from a meta-analysis that the effects of openness to change values on rule-breaking vary in direction, significance, and effect size, depending on the context. Openness-to-change values are positively related to the tendency to take risks (Weinstein et al. 2020). In our infosec context, we hypothesize that openness to change impacts ISP compliance in the opposite direction of conservation values, depending on the specific ISP under evaluation, because of the bipolar definition of the values construct that forces it to go in the opposite direction of conservation.

Hypothesis 2. *Openness-to-change values influence compliance with ISPs in the opposite direction of conservation values.*

Self-enhancement prioritizes values that motivate people to highlight their personal interests, including values of power and achievement. Self-enhancement values pursue control, dominance, and personal success (Schwartz et al. 2012), suggesting that a person with self-enhancement values may act with little consideration of society's ethical or moral codes (Feldman et al. 2015).

The theory of personal values' circumplex structure predicts the motivation underlying unethical behaviors. Furthermore, self-enhancement works as a motivator for rule-breaking (Feldman et al. 2015). We propose that self-enhancement is negatively related to compliance with ISPs because of the tendency to prioritize individual benefits even at the cost of disregarding ethical behaviors (Feldman et al. 2015), which, in the case of ISPs, translates into noncompliance.

Hypothesis 3. *Individuals who prioritize self-enhancement values do not comply with ISPs.*

Self-transcendence promotes values that motivate people to be unselfish and look for benefits that can be generally distributed between relatives, others, and society in general (Schwartz 1992). Self-transcendence "expresses the motivations for empathy, justice, and fairness toward others" (Feldman et al. 2015, p. 71). Therefore, self-transcendence avoids harm to others even against an individual's own benefit. In the case of ISP compliance, we expect self-transcendence values to be positively related to obeying rules or avoiding breaking them when others could potentially be harmed. In this case, we hypothesize that self-transcendence values are contrary to self-enhancement values because of the bipolar definition of the values construct that forces it to go in the opposite direction of self-enhancement.

Hypothesis 4. *Individuals who prioritize self-transcendence values comply with ISPs.*

Bardi and Schwartz (2003) found that social or peer pressure can strengthen or weaken the relationship between values and behaviors. Moreover, when testing the values-behaviors relationship, Schwartz et al. (2017) found partial support for this relationship and called for further research on the conditions under which social factors (normative pressure) moderate the relationship between values and intentions to behave. In the infosec literature, there have been calls to deepen the study of the interaction between social norms and personal values when comparing intrinsic and extrinsic motivators of ISP compliance (Malhotra et al. 2008). We expect the relationship between values and ISP compliance to be moderated by social factors.

Hypothesis 5. *Social factors moderate the relationship between personal values and ISP compliance.*

Research in human resources and remote work environments has found significant differences between remote and onsite employees. In particular, the life satisfaction of onsite workers is mediated by job satisfaction, but this is not the case for remote workers (Gillet et al. 2022). Furthermore, personality traits, such as conscientiousness and openness to experience, are associated with preference for teleworking and higher remote work productivity, but extroverted employees prefer working onsite (Gavoille and Hazans 2022). We posit that in the infosec context, personal characteristics, such as personal values, are more relevant in less controlled environments, such as remote work environments. Thus, we hypothesize that the relationship between personal values and ISP compliance is different for people primarily working from home compared with people primarily working onsite.

Hypothesis 6. *The relationship between personal values and compliance with ISPs differs between remote workers and onsite workers.*

Research Methodology

For our study, we utilized a scenario method (n = 352) to test the hypotheses. Prior to doing so, we conducted a pilot study (see Online Appendix 1) during the COVID-19 global lockdown in June 2020, when most workers were remote. The purpose of the pilot study was to establish whether personal values affected compliance intentions in remote environments. Our main study was conducted after hybrid work stabilized and became the new normal (McKinsey 2023). With the increased number of workers having the opportunity to work remotely, our study was designed to compare remote and onsite work settings to determine the implications for ISP compliance.

The scenario method is commonly used in the infosec literature because of its advantages in analyzing ISP violations. In this method, participants are presented with a description of a realistic hypothetical situation and important details regarding behavioral intentions, followed by a survey requesting responses to measure the variables of interest (Vance et al. 2013, 2015). The hypothetical scenario enhances the realism of the situation presented and allows researchers to measure intentions to do something that may be considered ethically or professionally incorrect (Vance et al. 2013, 2015). For our study, such a scenario was the critical element to be included, and it had to be equally realistic for both onsite and remote workers. The steps we followed to design our scenario are summarized in Online Appendix 2.

After creating the scenario, we designed the survey based on our findings from the pilot study. We pretested the scenario and survey with students in an introductory infosec class taught at a large private university located in the southern part of the United States. We received 90 responses, which allowed us to check the psychometric properties of the survey and make minor adjustments. After making all minor corrections, we proceeded with the primary data collection. Participants were recruited using Prolific, an online crowdsourcing platform, and data were collected through an anonymous Qualtrics survey. Prolific is recommended in the behavioral sciences for data collection (Peer et al. 2022).

Participants were compensated $3 for their voluntary participation in the study. Using Prolific's preset filters, we were able to restrict the subject pool to

employed workers based in the United States. In addition, Prolific prescreens respondents to guarantee that they fulfill the characteristics of the requested sample. In our case, potential participants were screened by Prolific to ensure that they were employed for at least 30 hours per week. They could work for a small or medium-size enterprise, a large private organization, or a publicly listed organization but with at least 50 employees. Participants needed to use information technology (IT) at least two or three times per week and, in all cases, no less than 30% of their time at work.

Participants were given a URL for the survey. When participants clicked on the survey invitation, they saw a welcome screen outlining the research and were asked for their consent to participate. If participants agreed, they were invited to read the scenario and imagine themselves in such a situation. After reading the assigned scenario, participants were presented with a questionnaire containing the variables of interest for this study contextualized to the scenario. The survey properties were set to allow participants to leave any items blank, read ahead in the questionnaire before completing items, and return to prior questions. As an important step, Prolific returns a response to the pool when there are concerns about data quality (e.g., missed attention checks).

Measures

For the personal values construct, we adapted the Higher-Order Value Scale (HOVS) developed by Lechner et al. (2024) and used in the GESIS Panel,[1] a European social science data infrastructure. The HOVS was developed to provide a parsimonious, valid, and reliable measure to reflectively assess the four higher-order values and to enable analyses based on observed scores and latent variables for each higher-order variable. Personal values (Schwartz 1992) have commonly been used to establish group differences in the relationship between values and behaviors (Sagiv and Schwartz 2022). The theory and the measure we used to establish group differences have been found to have structural validity and measurement invariance across groups, making them ideal for group comparison (Lechner et al. 2024).

For all other constructs, we used items similar to those in the studies by Moody et al. (2018). As an additional step, we included two attention checks as a primary instrument-validation principle (Boudreau et al. 2001). We also included a blue attitude construct (Miller and Chiodo 2008) as a marker variable to control for common method bias (CMB) (Simmering et al. 2015). All of the constructs were adapted to the infosec scenario by ensuring similar meanings across contexts (Hong et al. 2014, Crossler et al. 2018). The items used in this study can be found in Online Appendix 3.

Analysis

For our data analysis, we used SmartPLS 4.1 (Ringle et al. 2022) to analyze the measurement and structural models. We also executed a multigroup analysis (MGA) (Sarstedt et al. 2011). The MGA presents the difference of group-specific results based on bootstrapping (Sarstedt et al. 2011). As illustrated in Online Appendix 4, to assess the measurement model, we tested the measures' reliability, convergent validity, discriminant validity, and collinearity (Lowry and Gaskin 2014, Hair et al. 2016). To assess the structural model, we used bootstrapping with 5,000 samples.

Results

We collected a total of 361 responses, of which 352 remained after removing respondents who had missed attention-check questions or had timed out. The majority (58%) of participants were male. Their average age was 40 years, ranging from 20 to 70 years. Furthermore, 195 participants worked onsite more than 50% of the time, whereas 157 participants worked remotely more than 50% of the time. More than 95% of participants finished high school, with the majority of respondents (51.1%) holding a bachelor's degree.

The first assessment of the measurement model indicated that a few constructs demonstrated poor reliability. To increase the reliability of the constructs, we dropped one item from conservation (3), one item from the reactance measure (1), one item from self-enhancement (3), and one item from the social factors measure (1). After these changes, the composite reliability values for all of the constructs were above 0.70.

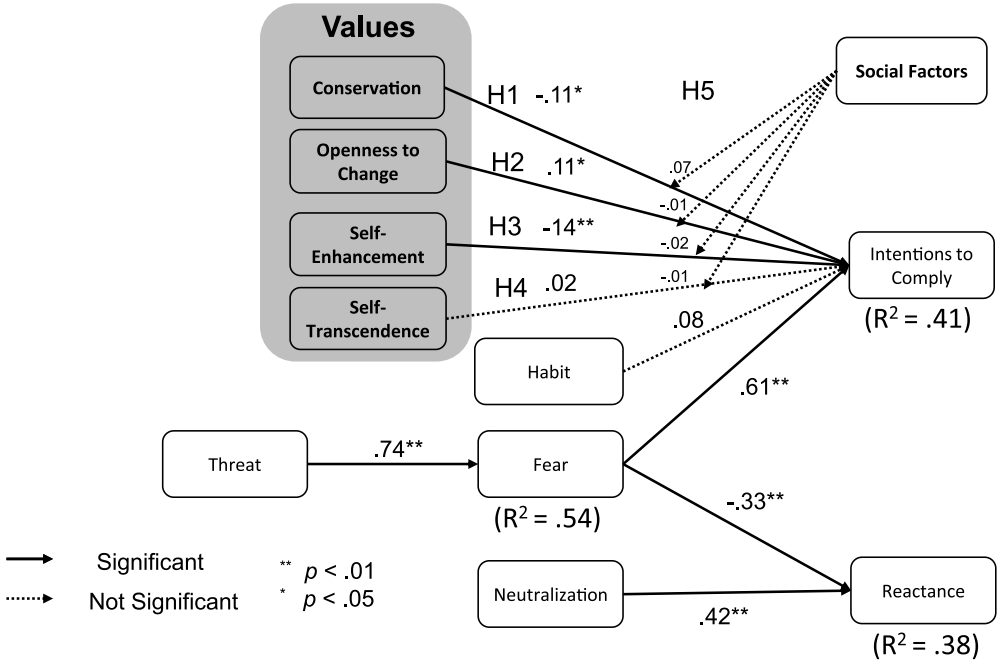
All of the constructs met the conditions for discriminant validity. For discriminant validity, we examined the individual item cross-loadings, which were all less than the constructs' loadings. We also compared the shared variance between constructs in relation to the shared variance between each construct and its own measures (Fornell and Larcker 1981). In this case, all constructs met the conditions for discriminant validity. For discriminant validity, the heterotrait-monotrait (HTMT) ratio can be used as well, and none of the values should exceed the 0.85 threshold (Henseler et al. 2015).

We found mixed results for the hypotheses in the research model (Figure 2).

Remote vs. Onsite Group Comparison

We split the full sample into two groups to evaluate H6, which is related to the differences between onsite and remote workers. Group 1 worked onsite more than 50% of the time (n = 195), and Group 2 worked

Figure 2. Results



remotely more than 50% of the time ($n = 157$). A comparison between groups using Structural Equation Modeling (SEM) represents a categorical moderating effect (Sarstedt et al. 2011). In our case, the categorical variable we used to test the moderating effect was group membership, by grouping users depending on whether a worker spent more or less than 50% of their time working remotely. The results for both groups are shown in Figure 3.

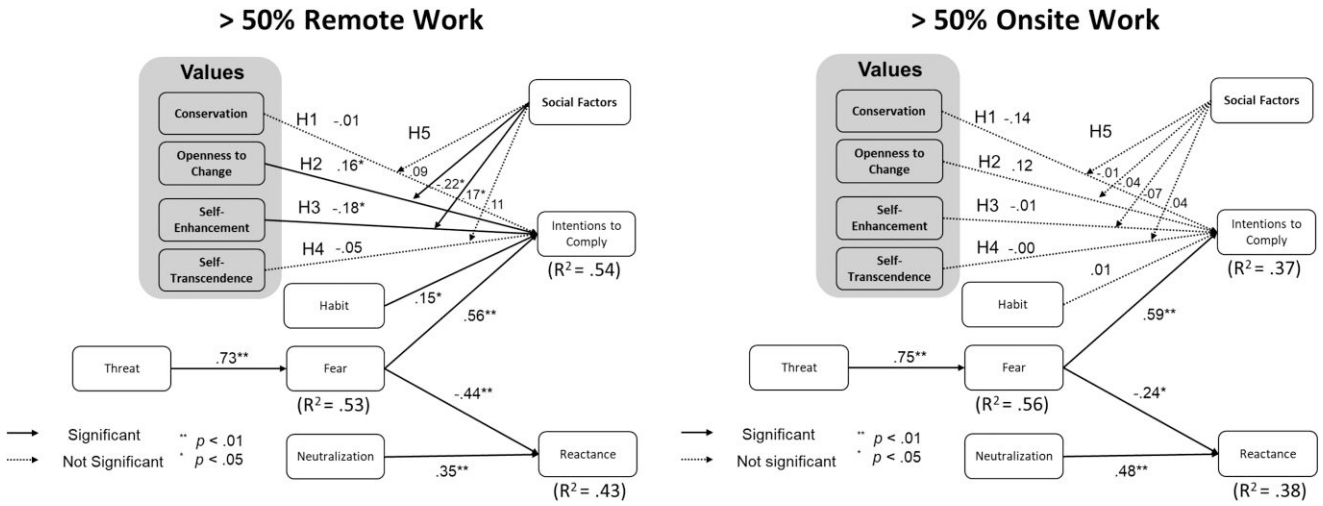
Discussion

Our research yields important implications for theory and practice. Prior research has emphasized the need to use more comprehensive theories to explain how values affect ISP compliance (Chu et al. 2019) beyond the traditional use of Hofstede's national values (Hofstede 1983) in cross-cultural research (see, e.g., Zhang and Lowry 2009 and Crossler et al. 2019). Overall, our research supports the notion that values play a role in ISP compliance, offering theoretical support to a statistically derived proposition by Moody et al. (2018). In addition, our study supports claims that organizations should consider ISP design and enforcement approaches that integrate employees' personal and psychological factors (Whitty et al. 2024). The support for H1, H2, and H3 extends and enhances the UMISPC by introducing personal values as direct and substantive predictors of ISP compliance behaviors. In particular, our research reveals that conservation (H1), openness-to-change (H2), and self-enhancement (H3) values are effective predictors of ISP compliance behaviors.

Our research is the first project in the rich infosec behavioral literature to provide empirical evidence that remote workers and onsite workers have different motivators to perform infosec behaviors. In general, our results suggest that personal values become more relevant motivators for workers working from home more than 50% of the time. The results of our group comparison provide partial support for H6, suggesting that remote/onsite work is a categorical moderator of the relationships between openness to change and ISP compliance and between self-enhancement and ISP compliance. In addition, our results offer support for three-way interactions (moderated moderation) in which the relationships between openness to change-ISP compliance and self-transcendence-ISP compliance are strengthened by social factors (H5) only in remote work conditions (H6).

Furthermore, our study suggests that personal values are especially substantive and relevant for ISP compliance in the context of remote work. In the pilot study (Online Appendix 1), the total variance in ISP compliance intentions explained by the model (R^2) was 0.44. Out of the total variance, 0.23 was due to the personal values. This result implies that the effect of values on compliance intentions in remote work environments was substantive because more than half of the total explained variance was due to the

Figure 3. Between-Groups Results



presence of the four personal values constructs in the model. In our main study, designed to compare workers working onsite most of the time with workers working remotely most of the time, the R^2 of ISP compliance intentions for the onsite work group (Group 1) was 0.37 (Figure 3). However, the R^2 for the group of remote workers (Group 2) was 0.54 (Figure 3). The 17% difference in explained variance between Group 1's R^2 and Group 2's R^2 suggests that this theoretical model is a better predictor for remote workers than for onsite workers. Because personal values were only a predictor of compliance behaviors for remote workers, we ran the model without the four personal values constructs and calculated an R^2 of 0.46. This represents 8% more variance explained for remote workers when values are added to the traditional UMISPC model. Given that the UMISPC was developed based on the consideration of numerous theories, the fact that this much more variance was explained by values demonstrates the substantive nature of including personal values along with the UMISPC theory.

The results of our study support the claim that remote employees demonstrate different levels of ISP compliance intentions compared with onsite employees (Felstead and Henseke 2017, Nyarko and Fong 2023). Furthermore, our research suggests that personal factors (Whitty et al. 2024), such as personal values (Schwartz 1992), affect remote workers' comprehension and acceptance of ISPs. Humans are viewed as the weakest link in the cybersecurity industry (Perez 2022). However, although humans may be the weakest link, they are also the first line of defense against cyberattacks, so employees need to be motivated and alert to protect information assets. Our research supports claims that organizations should consider and improve cybersecurity solutions by following recommendations to avoid cybersecurity programs that take a one-size-fits-all approach. (Whitty et al. 2024). Instead, they should tailor-make programs for individuals that take into account the different personal values that may be more appropriate given their work locations.

The need for tailor-made cybersecurity programs is more evident in the case of remote workers. The difference highlighted in our study between onsite and remote workers indicates that to circumvent a "my house, my rules" attitude toward cybersecurity, organizations may need to redesign and reevaluate cybersecurity programs, considering personal characteristics in their individualized solutions. This endeavor should be done in addition to and not separate from more traditional elements related to promoting and enforcing secure behaviors, such as fear appeals (Johnston and Warkentin 2010, Boss et al. 2015). Tailor-making ISPs requires significant knowledge about employees and a great amount of effort and expertise from organizations (Nyarko and Fong 2023). Understanding employees' personal values systems may help reduce the effort required while improving the results. Furthermore, managers should also try to identify how the different personal values present in the workforce can be understood to promote the proper use of IT tools, particularly ISPs mandated by organizations. For instance, knowledge of what personal values are important to any employee can be used to customize or personalize ISPs and communication campaigns that promote secure behaviors to foster compliance with ISPs.

Although personal values are important, our findings provide more nuanced insights into the effects that different values have on intentions to comply. In

particular, conservation had a significant negative effect on intentions to comply ($\beta = -0.107$, $p = 0.028$), supporting H1. Interestingly, this result seems to be driven by onsite workers because in the group comparison, conservation had a higher beta-value in the onsite group, even though it was nonsignificant ($p = 0.068$). The lack of significance could be due to a lack of power, so future research can be conducted to understand the relevance of conservation values in onsite settings. Prior personal values research has found that those who hold conservation values and are thus motivated by respect for tradition and authority can break rules if those rules do not align with their traditional way of thinking, implying important changes in how they traditionally behave if authority is challenged or diminished (Sagiv and Schwartz 2022). Our results are consistent with this research given that in the hypothetical situation, our participants were making decisions related to a request from a manager on behalf of a vice president, both of whom would be considered authority figures. Conservation values value authority, and in this case, most people would perceive the request as an order to be accepted and fulfilled. Furthermore, considering that onsite work is the traditional work setting, employees driven by conservation values may have an understanding that cybersecurity is an organization's responsibility rather than a personal responsibility. To switch the direction of this relationship, organizations and managers can take advantage of understanding employees with conservation values by emphasizing the role of authority not in breaking rules but in submitting to them.

We also found that openness to change positively impacted compliance with ISPs ($\beta = 0.104$, $p = 0.028$), supporting H2. Because openness to change is bipolar to conservation in relation to the behaviors under study (Sagiv and Schwartz 2022), our result is consistent with the general tenet of the theory of personal values (Schwartz et al. 2012) and can be explained by the fact that hybrid work became a novel and sought-after workstyle after the pandemic. Individuals who hold openness-to-change values are driven by the excitement of novelty and freedom to determine their actions and make their own choices (Sagiv and Roccas 2021, Sagiv and Schwartz 2022). In the infosec context, with more remote work accepted by organizations, those employees who value openness to change are likely interested in taking advantage of any opportunity to increase the amount of time they can work from home. Furthermore, our findings are consistent with research showing that people with personalities characterized by openness to new experiences are better suited for remote work (Gavoille and Hazans 2022). Those who hold openness-to-change values may see compliance with ISPs as an excellent way to retain that gained freedom. The new standard of and novelty in remote work may have created a high sense of morality and responsibility toward organizations, motivating remote employees to be more conscious of cyberthreats and thus increase their compliance. Organizations may benefit by understanding that innovation and freedom motivate employees driven by openness to change. Policies and communications directed to this group should emphasize that compliance increases freedom and that employees' ideas will always be considered in how they can act to protect organizations' information assets.

Another important factor to consider is that self-enhancement values, which privilege a personal view, achievement, and power, had a negative effect on ISP compliance ($\beta = -0.139$, $p = 0.025$), supporting H3. Those who hold self-enhancement tend to engage in negative behaviors if those behaviors are personally rewarding (Schwartz 1992, Sagiv and Schwartz 2022). Holders of self-enhancement values demonstrate competence and are in constant search of personal success and power, so they are purely motivated by what they can obtain from their behaviors (Schwartz 1992, Sagiv and Schwartz 2022). In the scenario presented in this study, a manager requested that a rule be broken to help a vice president. Thus, a person driven by self-enhancement values could identify violating a policy to satisfy their manager and a vice president as an opportunity to gain recognition and continue escalating in his or her career. This effect could be even more pronounced in a remote environment because the chance to get recognized by a vice president would be scarcer. Thus, for IT managers, our study highlights the importance of understanding self-driven and personal-oriented workers, so they should present ISPs as an element of personal gain rather than a more general or organizational benefit. When workers driven by such values understand that ISPs can produce immediate rewards, they will be more likely to comply with them.

Self-transcendence values (universality and benevolence) did not significantly affect ISP compliance, failing to support H4. This finding is consistent with the fact that people who think in a way that allocates importance to general benefit over individual gain prioritize behaviors that benefit the society they are part of (Schwartz et al. 2012). In the context of our research, there was no clear benefit to the group, society, or even the organization that would motivate a self-transcendent person toward either compliance or noncompliance. Furthermore, remote work may create a distant relationship with and disconnection from the organization, so there is little general benefit perceived in ISP compliance.

The moderating effect of social factors on the different values was significant only in the remote work group, which constitutes a moderated moderation relationship

(Hayes 2018), providing limited support for H5. The three-way interactions involved social factors moderating the relationship between openness to change and compliance in the remote work group ($\beta = 0.022$, $p = 0.011$) as well as the relationship between self-enhancement and compliance ($\beta = 0.172$, $p = 0.037$). This finding supports values researchers' claim that the relationship between individualism-oriented types of values (openness to change and self-enhancement) and behaviors can be strengthened, depending on the type of cohesion in a group and whether all group members act accordingly (Sagiv and Schwartz 2022).

Four of the five relationships kept from the UMISPC were supported (Figures 2 and 3), and the fifth (habit) was supported only in remote work environments. Even though we add predictive power to the model by introducing the theory of personal values, we acknowledge that traditional and well-researched strategies, such as fear appeals (Johnston and Warkentin 2010, Boss et al. 2015), are effective and need to be included in infosec compliance promotional strategies by managers. Our study indicates that fear is still an important factor when it comes to ISP compliance and is fully applicable in both onsite and remote work environments. Oddly, in Moody et al.'s (2018) results, the relationship between fear and intentions to comply was negative, whereas the relationship between fear and reactance was positive. The directions of those relationships in Moody et al.'s (2018) work are counterintuitive and were unexplained. In the present study, fear positively influenced intentions to comply, which is consistent with extant infosec empirical research (Boss et al. 2015), and it negatively affected reactance (Siponen and Vance 2010). The other relationships from the UMISPC (Moody et al. 2018), such as threat as a positive predictor of fear (Boss et al. 2015) and neutralization and fear as motivators for reactance (Siponen and Vance 2010), were consistent with previous ISP compliance research.

The final relationship tested by the UMISPC was between habit and intentions to comply. In our case, in support of Moody et al.'s (2018) model, habit significantly influenced intentions to comply with the ISP, but only in the remote work group. We acknowledge the difficulties brought by contextual factors that can potentially modify the explanatory power of the different ISP compliance research models. We speculate that the reason why habit was supported only in the remote work group is because in order for compliance to become a daily routine, a lot of self-discipline and constant practice are required. Such behaviors occur only in self-satisfied and conscientious employees (Gavoille and Hazans 2022, Gillet et al. 2022) who put the training they have received into practice (Nyarko and Fong 2023), which characterizes most remote employees. In this case, we believe that organizations should not only train people on cybersecurity practices but also offer regular opportunities to practice until those practices become the standard and natural behavior.

Limitations and Future Research

Our findings come from an individual perspective, like much of the compliance literature. The focus of this literature is often on individuals' compliance with ISPs. Other research has taken the organization's perspective, in which the objective is to maximize the organizational benefits, suggesting that accepting a certain amount of risk is cost-beneficial to organizations. Thus, noncompliance cannot be eliminated entirely, or it would be too costly (Dey et al. 2022). Our research contributes to the general compliance literature by introducing the theory of personal values that can be used at multiple levels of analysis (Rohan 2000). Future research should try to balance understanding individual behaviors with maximizing what is needed for organizations. Employees with different values can be part of different teams in a way that balances both personal and organizational values and their motivated behaviors to improve organizational results. Furthermore, understanding how the different values influence behaviors in multiple different scenarios offers potential opportunities to build on what this study demonstrates.

Furthermore, we measured intentions to comply instead of actual compliance with ISP. We acknowledge multiple calls from scholars to study actual security behaviors (Crossler et al. 2013, Lowry et al. 2017). Future research based on secondary data could determine whether individuals' factors effectively prevented realized security events. Experimental research can also be conducted by exposing individuals who hold different values to real scenarios and measuring their actual compliance.

Our cross-sectional research did not allow us to account for the important effect of time in ISPs. Future longitudinal research is warranted to identify the type of interventions and the effect of time in modifying the individual's values priorities and its relationship with ISP compliance. Such studies would offer clarity on several topics, such as the effect of time on compliance and the implications of values in neutralization techniques, shedding light on potential elements that may foster positive or adverse reactions toward ISPs.

As research on ISP compliance moves forward, establishing the context of work environments is important to fully understand the factors that lead to compliance. In particular, when remote work is considered, including personal values in the theoretical model will be important to fully capture differences in compliance.

Endnote

[1] https://www.gesis.org/en/gesis-panel/gesis-panel-home.

References

Bardi A, Schwartz SH (2003) Values and behavior: Strength and structure of relations. *Pers. Soc. Psychol. Bull.* 29(10):1207–1220.

Boss S, Galletta D, Lowry PB, Moody GD, Polak P (2015) What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quart.* 39(4):837–864.

Boudreau M-C, Gefen D, Straub DW (2001) Validation in information systems research: A state-of-the-art assessment. *MIS Quart.* 25(1):1–16.

Chu X, Luo XR, Chen Y (2019) A systematic review on cross-cultural information systems research: Evidence from the last decade. *Inform. Management* 56(3):403–417.

Cieciuch J, Davidov E, Vecchione M, Beierlein C, Schwartz SH (2014) The cross-national invariance properties of a new scale to measure 19 basic human values: A test across eight countries. *J. Cross Cult. Psychol.* 45(5):764–776.

Cisłak A, Wójcik A, Białobrzeska O (2022) Social position and personal vs. social focus: A multinational study of managerial values. *Soc. Psychol. Bull.* 17:1–26.

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.

Crossler RE, Andoh-Baidoo FK, Menard P (2019) Espoused cultural values as antecedents of individuals' threat and coping appraisal toward protective information technologies: Study of US and Ghana. *Inform. Management* 56(5):754–766.

Crossler RE, Di Gangi PM, Johnston AC, Bélanger F, Warkentin M (2018) Providing theoretical foundations: Developing an integrated set of guidelines for theory adaptation. *Comm. Assoc. Inform. Systems* 43(1):566–597.

Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R (2013) Future directions for behavioral information security research. *Comput. Secur.* 32:90–101.

Dey D, Ghoshal A, Lahiri A (2022) Circumventing circumvention: An economic analysis of the role of education and enforcement. *Management Sci.* 68(4):2914–2931.

Elo J, Lumivalo J, Tuunanen T (2022) A personal values-based approach to understanding users' co-creative and co-destructive gaming experiences in augmented reality mobile games. *Pacific Asia J. Assoc. Inform. Systems* 14(5).

Feldman G, Chao MM, Farh J-L, Bardi A (2015) The motivation and inhibition of breaking the rules: Personal values structures predict unethicality. *J. Res. Pers.* 59:69–80.

Felstead A, Henseke G (2017) Assessing the growth of remote working and its consequences for effort, well-being and work-life balance. *New Technol. Work Employ.* 32(3):195–212.

Fornell C, Larcker DF (1981) *Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics* (SAGE Publications, Thousand Oaks, CA).

Frimer JA, Walker LJ (2009) Reconciling the self and morality: An empirical model of moral centrality development. *Developmental Psych.* 45(6):1669–1681.

Gavoille N, Hazans M (2022) Personality traits, remote work and productivity. IZA Discussion Paper, No. 15486, Institute of Labor Economics (IZA), Bonn.

Gillet N, Morin AJS, Huyghebaert-Zouaghi T, Austin S, Fernet C (2022) How and when does personal life orientation predict well-being? *Career Development Quart.* 70:240–255.

Greulich M, Lins S, Pienta D, Thatcher JB, Sunyaev A (2024) Exploring contrasting effects of trust in organizational security practices and protective structures on employees' security-related precaution taking. *Inform. Systems Res.* Forthcoming.

Hair JF, Hult GTM, Ringle C, Sarstedt M (2016) *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)* (Sage publications, Thousand Oaks, CA).

Hayes AF (2018) Partial, conditional, and moderated moderated mediation: Quantification, inference, and interpretation. *Commun. Monogr.* 85(1):4–40.

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

Hofstede G (1983) National cultures in four dimensions: A research-based theory of cultural differences among nations. *Int. Stud. Manage. Organ.* 13(1–2):46–74.

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

IBM (2023) Cost of a data breach report. Accessed January 14, 2024, https://www.ibm.com/reports/data-breach.

Johnson V, Torres R, Maurer C, Guerra K, Srivastava S, Mohit H (2023) The 2022 SIM IT issues and trends study. *MIS Quart. Executive* 23(1):86–124.

Johnston AC, Warkentin M (2010) Fear appeals and information security behaviors: An empirical study. *MIS Quart.* 34(3):549–566.

Lechner C, Beierlein C, Davidov E, Schwartz SH (2024) Measuring the 4 higher-order values in Schwartz's theory: A validation of a 17-item inventory. *J. Pers. Assess.* 1–14.

Lowry PB, Gaskin J (2014) Partial Least Squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE Trans. Prof. Commun.* 57(2):123–146.

Lowry PB, Dinev T, Willison R (2017) Why security and privacy research lies at the centre of the Information Systems (IS) artefact: Proposing a bold research agenda. *Eur. J. Inform. Systems* 26(6):546–563.

Malhotra Y, Galletta DF, Kirsch LJ (2008) How endogenous motivations influence user intentions: Beyond the dichotomy of extrinsic and intrinsic user motivations. *J. Management Inform. Systems* 25(1):267–300.

McKinsey GI (2023) How hybrid work has changed the way people work, live, and shop. Accessed January 14, 2024, https://www.mckinsey.com/mgi/our-research/empty-spaces-and-hybrid-places-chapter-1#/.

Miller B, Chiodo B (2008) Academic entitlement: Adapting the equity preference questionnaire for a university setting. *Southern Management Association Meeting, St. Pete Beach, FL.*

Moody GD, Siponen M, Pahnila S (2018) Toward a unified model of information security policy compliance. *MIS Quart.* 42(1): 285–311.

Nyarko DA, Fong RC-w (2023) Cyber security compliance among remote workers. Jahankhani H, ed. *Cybersecurity in the Age of Smart Societies* (Springer International Publishing, Springer, Cham, Switzerland), 343–369.

Peer E, Rothschild DM, Evernden Z, Gordon A, Damer E (2022) Data quality of platforms and panels for online behavioral research. *Behavioral Res. Methods* 54:1643–1662.

Perez C (2022) Your employees are the weakest link in your cybersecurity chain (EY Cybersecurity Series, Issue). Accessed August 18, 2023, https://www.ey.com/en_ca/cybersecurity/your-employees-are-the-weakest-link-in-your-cybersecurity-chain.

Rahamti M (2023) How to navigate cybersecurity risks in the era of remote work. *The CEO Magazine* (October 16). https://www.theceomagazine.com/opinion/cybersecurity-threats/.

Ringle CM, Wende S, Becker JM (2022) SmartPLS 4. *Oststeinbek: SmartPLS*. https://www.smartpls.com.

Rohan MJ (2000) A rose by any name? The values construct. *Pers. Soc. Psychol. Rev.* 4(3):255–277.

Sagiv L, Roccas S (2021) How do values affect behavior? Let me count the ways. *Pers. Soc. Psychol. Rev.* 25(4):295–316.

Sagiv L, Schwartz SH (2022) Personal values across cultures. *Annu. Rev. Psychol.* 73:517–546.

Sarstedt M, Henseler J, Ringle CM (2011) Multigroup analysis in partial least squares (PLS) path modeling: Alternative methods and empirical results. *Measurement and Research Methods in International Marketing* (Emerald Group Publishing Limited, Bingley, UK), 195–218.

Sarstedt M, Hair JF Jr, Cheah J-H, Becker J-M, Ringle CM (2019) How to specify, estimate, and validate higher-order constructs in PLS-SEM. *Australas. Marketing J.* 27(3):197–211.

Schwartz SH (1992) Universals in the content and structure of values: Theoretical advances and empirical tests in 20 countries. Zanna MP, ed. *Advances in Experimental Social Psychology*, vol. 25 (Academic Press, New York), 1–65.

Schwartz SH (1994) Are there universal aspects in the structure and contents of human values? *J. Soc. Issues* 50(4):19–45.

Schwartz SH, Cieciuch J, Vecchione M, Torres C, Dirilem-Gumus O, Butenko T (2017) Value tradeoffs and behavior in five countries: Validating 19 refined values. *Eur. J. Soc. Psychol.* 47:241–258.

Schwartz SH, Cieciuch J, Vecchione M, Davidov E, Fischer R, Beierlein C, Ramos A, Verkasalo M, Lönnqvist JE, Demirutku K (2012) Refining the theory of basic individual values. *J. Personality Soc. Psychol.* 103(4):663–688.

Simmering MJ, Fuller CM, Richardson HA, Ocal Y, Atinc GM (2015) Marker variable choice, reporting, and interpretation in the detection of common method variance: A review and demonstration. *Organ. Res. Methods* 18(3):473–511.

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

Tams S, Dulipovici A, Thatcher JB, Craig K, Srite M (2020) The role of basic human values in knowledge sharing: How values shape the postadoptive use of electronic knowledge repositories. *J. Assoc. Inform. Systems* 21(1):201–237.

Vance A, Lowry PB, Eggett D (2013) Using accountability to reduce access policy biolations in information dystems. *J. Management Inform. Systems* 29(4):263–290.

Vance A, Lowry PB, Eggett DL (2015) Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations. *MIS Quart.* 39(2):345–366.

Verizon (2023) 2023 data breach investigation report. Accessed January 14, 2024, https://www.verizon.com/business/resources/reports/dbir.

Weinstein Z, Roccas S, Gandal N (2020) Personal values and cyber risk-taking. Preprint, submitted October 18, 2020, http://dx.doi.org/10.2139/ssrn.3714173.

Whitty MT, Moustafa N, Grobler M (2024) Cybersecurity when working from home during COVID-19: Considering the human factors. *J. Cybersecurity* 10(1):1–11.

Zhang D, Lowry PB (2009) Issues, limitations, and opportunities in cross-cultural research on collaborative software in information systems. *E-Collaboration: Concepts, Methodologies, Tools, and Applications* (IGI Global, Hershey, PA), 553–585.