Issues in Information Systems
Volume 25, Issue 2, pp. 346-362, 2024

DOI: https://doi.org/10.48009/2_iis_2024_128

To follow the rules or break them: An individual rule-following perspective

Darin Hodges, *Appalachian State University, hodgesdc@appstate.edu*
Russell Haines, *Appalachian State University, hainesrp@appstate.edu*
Deepti Agrawal, *California State Polytechnic University, dr.agrawald@gmail.com*

Abstract

Most security breaches are caused by human error, and employees are perceived as the last line of defense against threats that have evaded technological controls by network administrators. Accordingly, organizations invest in information security policy (ISP) creation, implementation, and training initiatives to train employees to recognize and evade security threats. Generally, ISPs are meant to clarify employees' information security decisions and take time to develop and implement. However, many policies are slow to adapt and guide employees as work conditions change or new technologies are introduced to increase productivity and gather and share data to perform work-related activities. Despite much research on what motivates employee security policy behavior, we have yet to determine why employees continue to fail to prevent malicious actions against organizational information systems. Many ISP compliance studies articulate an 'all or nothing' approach to ISPs, which assumes the policies are written to cover all possible decisions employees may perform concerning information security. Unfortunately, we argue this is not justified as employees face new and novel approaches from malicious actors and technologies meant to undermine the rules put in place through the ISP. We also argue that it is not enough to study the motivations behind ISP compliance since motivations can be nuanced and different for adaptive behavior (ISP compliance) as opposed to maladaptive behaviors (avoidance and non-compliance). Therefore, we take a rule-following perspective to study both. We argue that when the requirements of ISP disrupt their work, employees face rule tension. In response to rule tension, they are less likely to exhibit adaptive behaviors and more likely to exhibit maladaptive behaviors. In addition, we propose that two common governance approaches- (1) command-and-control and (2) self-regulatory moderate the relationship between rule tension and adaptive and maladaptive behaviors in the context of ISP rule-following.

Keywords: ISP compliance, information security, adaptive security behavior, maladaptive security behavior, rule-following

Introduction

Industry reports indicate that about 74% of cybersecurity breaches began through human error, social engineering, or misuse (Verizon, 2023), implying that employees remain the biggest threat to information security. Cyber-attacks on organizations are growing in sophistication, and cybersecurity professionals find it difficult to keep up with increasingly complex systems that provide a barrier between information security threats and non-technical employees (Splunk, 2023). The routine interaction between the employees and the organization's systems and data can both create vulnerabilities or help safeguard the organization's security efforts. Recognizing this, most organizations have invested in implementing information security

policies (ISP) and training to make employees their first line of defense against cyberattacks. However, the policies are only effective to the extent they are followed and/or adapted to changing threat vectors and novel technologies that provide employees with the guidance needed to perform work tasks. Employees face a dilemma when policies conflict with work requirements or have not adapted to integrate changing working environments. They must decide how to accomplish stated task goals while protecting organizational information systems and data.

A vast stream of research has examined factors motivating employee behaviors concerning information security policies. Adaptive behaviors aim to reduce or remove security threats, for instance, by taking defensive measures, and attempting to alleviate security threats through proactive action (e.g. ISP compliance). On the other hand, maladaptive behaviors focus on managing emotions triggered by security threats and avoiding decisions that could lead to positive organizational outcomes (e.g. ISP non-compliance, avoidance) (Chen et al., 2022). A few studies have suggested that an employee's motivations for adaptive behaviors may not be the same as those for maladaptive behaviors (Chen et al., 2022; Karjalainen et al., 2019), highlighting the pressing need for a more holistic approach that can account for both adaptive and maladaptive behaviors towards ISP.

Further, a recent investigation by Karjalainen et al. (2019) identified a possible cause of tensions in employee information systems security behavior as the differing goals and interests between individual employees and the organization. They postulated that this tension would lead individuals to balance environmental conditions or situational demands with compliant, partially compliant, or non-compliant decisions. While the theory was not tested, the investigation highlighted the need for further examination into ISP-related employee rule tensions.

In this study, we take a rule-following perspective, which defines rules as "explicit or implicit norms, regulations, and expectations that regulate the behavior of individuals and interaction among them" (Hannah & Robertson, 2015, p. 383). Conventional understanding of the information security policies closely matches the above definition of rules. Rule tension refers to 'an individual experience of tension which appeared to provide the fuel for employees to break or bend the rules causing the tension (Hannah & Robertson, 2015).

One reason behind the employees not following the organizational rules is that the requirements of the rules disrupt or impede their work (Bulgurcu et al., 2010; Hannah & Robertson, 2015). In circumstances where information security policy gets in the way of carrying out their work efficiently or effectively, the employees may experience rule tension. The employees may choose to follow the rules, break them, or find another way to reconcile the tension between the demands of the rules and their getting their work done.

Prior research (Siponen & Iivari, 2006; Yazdanmehr et al., 2020) indicates two prevalent rule enforcement strategies that align with the ISP governance strategies - (1) the command-and-control approach, a fear-based, coercive policy enforcement compliance strategy, and (2) the self-regulatory approach, which involves policy-making leaders justifying the policy. We propose these governance strategies as moderators of the relationship between rule tension and adaptive and maladaptive behaviors.
Considering recent information systems literature that underscores the need for more exploration of rule tensions in the workplace and their impact on adaptive as well as maladaptive ISP behavior, along with the limited research on governance strategies as moderators of relationships related to ISP behaviors, this study aims to address these research gaps.

This study aims to understand the mechanism behind the employee' decision to follow or go against the information security policies of their organizations when they face rule tension. More specifically we seek the answers to the following research questions:

> ***RQ1:*** *How does the rule tension influence an employee's behavior toward information security policy?*
>
> ***RQ2:*** *How do the command-and-control and the self-regulatory approaches influence an employee's behavior towards information security policy when faced with rule tension?*

Theoretical background and research model

Security-related stress (SRS) has been defined as an internal and/or external security-related demand that individuals experience when information security policies are perceived as being a burden to complete work or as a requirement that exceeds their resources or abilities. (D'Arcy et al., 2014). Tensions arise in individuals when attempting to adhere to the organization's stated information security-related policies while accomplishing work tasks (Calic et al., 2016; Parsons et al., 2013). The policy can become outdated and create stress for employees, including information overload, insecurity with the technology, novel complexities when adapting to the changing work environment, and overall uncertainty in how to integrate new technologies within existing guidelines to get work completed (Hwang & Cha, 2018).

Other impacts of SRS have been investigated, including the non-technical influences that information security policies have on employees. Ament and Haag (2016) found that SRS negatively affected employees' productivity, while neutralization has been researched as a coping mechanism to make excuses for violating organizational ISPs (D'Arcy et al., 2014). Hwang and Cha (2018) demonstrated that the creators of security-related technostress within organizations negatively impact employees' commitment to the organization, diminishing their intention to comply with ISPs.

D'Arcy and Lowry (2019) argued that the adverse emotions of frustration and fatigue produced by SRS strengthened the negative reactions to ISP compliance, making employees more inclined to use coping mechanisms, such as neutralization, to violate ISPs. Specifically, work-impediment events negatively affected daily attitudes toward ISP compliance intentions due to employees' belief that stated policies could interfere with daily job functions, creating difficulties (or stressors) in reaching work goals (D'Arcy & Lowry, 2019; Rodell & Judge, 2009). Previous research has indicated that work-impediment events can be created through technology use or disruptions to primary work tasks (Ayyagari et al., 2011; Gooty et al., 2014; Rodell & Judge, 2009). Such disruptions can occur at varying rates and degrees of recurrence and may include ISP requirements such as two-factor authentication, complex password requirements, or installation of security updates (D'Arcy et al., 2014; D'Arcy & Lowry, 2019; Posey et al., 2017).

Governance approaches to information security

Governance approaches are generally viewed through two lenses, command-and-control and self-regulatory, and are primarily utilized as antecedents to ISP compliance intentions or violations (Siponen & Iivari, 2006; Yazdanmehr et al., 2020). The command-and-control method involves enforcing regulations through rewards and punishments and setting up policies and procedures to identify violations of ISPs and is extrinsically motivated and is designed to inform individuals of the probability and consequences of getting caught for non-compliance. Command-and-control governance approaches are often associated with deterrence theory, which has historically been the primary theory of investigation concerning

employee compliance with ISP rules. Liu et al. (2018) examined the moderating effects of procedural justice and self-control on the links between perceived deterrence and benefits and IUP compliance intention but found that none of these variables significantly moderated the relationship. They discovered that employees with a higher stability meta-trait were more responsive to deterrence, while the effects of plasticity were mixed. Hovav and D'Arcy (2012) also studied the role of cultural differences in the effectiveness of deterrence in reducing IS misuse intention and found that the patterns for South Korean employees were opposite from those of United States employees. While extrinsically motivated factors such as deterrence have been studied extensively, there are indications that intrinsic self-regulated approaches to information security may be more effective (Son, 2011).

The self-regulatory approach posits that intrinsic desires, and for this study, the desire for security policy compliance, are the main drivers of behavior. This desire for compliance is based on two employee perceptions: value congruence and legitimacy (Tyler & Blader, 2005). Value congruence refers to the alignment of an employee's personal values with those of the organization (Kranz & Haeussinger, 2014; Malhotra et al., 2008; Tyler & Blader, 2005) while legitimacy pertains to the perception of the organization's leadership and rules as being valid and authoritative (Tyler, 2006). High-value congruence encourages compliance by allowing individuals to uphold their values while working for the organization. Similarly, the perceived legitimacy of superiors and organizational policies also promotes ISP compliance. Self-regulatory approaches also encompass other intrinsic mechanisms such as personal norms, moral beliefs, and moral commitments (D'Arcy et al., 2009). These mechanisms involving self-imposed punishments and rewards have been studied in relation to employee compliance. Personal norms and moral beliefs, which reflect an individual's commitment to personal values, are similar to the value congruence construct of the self-regulatory approach and imply that personal norms align with organizational values before individuals make positive compliance decisions (Cram et al., 2017; Yazdanmehr & Wang, 2016). For instance, denial of personal responsibility has been shown to moderate the effect of IS codes of ethics on deterring computer abuse intention. Similarly, the ascription of personal responsibility has been found to reinforce the impact of personal norms on compliance. These findings highlight the complex interplay of various factors in shaping compliance behavior within the self-regulatory approach.

Information security policy compliance and maladaptive behavior

Information security policies include rules, procedures, and guidelines governing the use and management of IT assets and resources, generally called information security policy compliance (Moody et al., 2018). Compliance is considered an adaptive coping response to an information security threat. Once individuals believe they have the necessary resources to counteract a threat, they can employ a strategy to lessen the effect and successfully mitigate the security risk (Chen et al., 2021). These threats are viewed as problems that can be solved when the individual has the necessary efficacy to deal with the threat successfully. ISPs are utilized to combat the problem at hand and comply with organizational policies. However, employees are often seen as the weakest link in information security (Bulgurcu et al., 2010), and their attitudes toward compliance can affect a company's cybersecurity policy and any technical measures deployed to deter would-be attackers. Despite knowing that compliance leads to safer interactions, employees often are reluctant to follow information security policies (Boss et al., 2009; Moody et al., 2018) for various reasons. Numerous studies have investigated the underlying issues as to why end users do not practice secure information security procedures and how to promote the best effective compliance (D'Arcy & Herath, 2011; Moody et al., 2018; Warkentin & Willison, 2009). These studies have generally overlooked the reasons for maladaptive compliance behaviors—focusing only on the dependent variable of ISP compliance and its antecedents. Maladaptive behavior occurs when employees fail to meet requirements associated with ISPs or generally seek to avoid problems associated with ISP compliance or obtaining the necessary skills to combat security threats (Cram et al., 2019; Posey et al., 2017).

Governance approaches have provided diverse findings and integrated many constructs that have either attempted to moderate or mediate the relationship between governance approaches and information security compliance (Moody et al., 2018). Employees in organizations generally have conflicting objectives and roles concerning work outcomes and goals, and complex security issues can arise unexpectantly (Hedström et al., 2013; Hedström et al., 2011; Karjalainen et al., 2019; Kolkowska & Dhillon, 2013). Hedström et al. (2011) theorized a value-based model that contrasts organizational policy goals, and values for employees regarding ISP compliance to employees' actions guided by their own rationalities, goals, and values when deciding whether to comply with ISPs. Research has supported that a

self-regulatory governance approach, which relies on shared security values and beliefs, is more effective for ISP compliance than a command-and-control approach (Li et al., 2014). When employees find themselves torn between competing goals (sometimes due to role conflict brought about by different management systems) and values, they are more likely to respond with maladaptive behaviors of non-compliance (Karjalainen et al., 2019). As a result, they may ignore organizational ISPs and choose maladaptive behaviors of non-compliance.

Many theories, such as rational choice theory, theory of planned behavior, control balance theory, protection motivation theory, and general deterrence theory have been utilized in these investigations of ISP compliance (Chen et al., 2018). Due to mixed results within the ISP compliance literature, there have been suggestions that the mixed results in security policy compliance research could be due to overlooked moderating or mediating variables (Chen et al., 2018; D'Arcy & Herath, 2011) or additional dependent outcomes such as avoidance or non-compliance (Chen et al., 2021). Additionally, Chen et al. (2021) noted that employees may change from compliance to non-compliance when problems associated with compliance become too great.

Hypothesis development and research model

Based on prior literature (D'Arcy et al., 2014; D'Arcy & Lowry, 2019; D'Arcy & Teh, 2019; Myyry et al., 2009), some of how employees may experience security-related stress is through 'rule tension' in the context of information security and may include slowing down their work due to IS policies (work obstruction tension), not being able to share information easily with people in their network (network tension), and lack of alignment between ISP and an employee's identity (identity tension). *Work obstruction tension* is related to ISP conflicts which make it difficult to complete work, initiate too many steps to comply with the policy, slow the pace of work, or diminish the quality of work (Hannah & Robertson, 2015). Rule tension associated with *engagement in networks* is related to policies that prevent the flow of information sharing. It could prevent the sharing of information with colleagues (internal network) and also to falling behind on technology, being left out of collaborations, or missing out on valuable feedback (external network). An employee faces *identity tension* when the rules outlined in the ISP do not align with the values or identity of the employees.

Bulgurcu et al. (2010)found that employees were less likely to comply with information system policies that hindered their work. Similarly, Hannah and Robertson (2015) discovered that employees responded more negatively to policies that disrupted their work than to coercive ones. Policies that interfere with operational and job-related tasks can create tension among workers and can create conflict with what employees reasonably expect regarding work disruption (Hannah & Robertson, 2015) and the rules governing work tasks. Employees may deviate from or disregard rules intended to safeguard confidential information due to conflicts between these rules and other expectations they encounter; employees typically manage this tension in a manner they believe benefits not only their personal interests but also the interests

of the organization they work for highlighting the probability of both adaptive and maladaptive behaviors (Hannah & Robertson, 2015). Hence, we hypothesize,

> ***H1:*** *Employees who perceive rule tension are less likely to exhibit adaptive behaviors toward ISP compliance.*
> ***H2:*** *Employees who perceive rule tension are more likely to exhibit maladaptive behaviors toward ISP compliance.*

The command-and-control approach assumes an economic view of human behavior and actions, indicating that people use a cost-benefit analysis to maximize benefits and minimize costs. Hence, employees will consider rewards associated with ISP compliance and sanctions for non-compliance in their decision to follow the rules or not. When faced with rule tension, employees are likely to break the rules to the point where the marginal benefit of getting their work by breaking the rule outweighs the cost of sanctions for breaking the rule. Hence, we hypothesize,

> ***H3a:*** *The command-and-control approach positively moderates the relationship between rule tension and adaptive behaviors.*
> ***H3b****: The command-and-control approach negatively moderates the relationship between rule tension and maladaptive behaviors.*

The self-regulatory approach to rule-following suggests that individuals will follow the rules due to internalization regardless of any external rewards or sanctions (Yazdanmehr et al., 2020). Employees are more likely to follow the rules through a self-regulatory approach if they perceive that the authorities who created the rules are legitimate. According to this approach, when faced with rule tension, employees are more likely to follow the ISP when they personally agree with and accept the policy. Hence, we hypothesize,

> ***H4a:*** *The self-regulatory approach positively moderates the relationship between rule tension and adaptive behaviors.*
> ***H4b****: The self-regulatory approach negatively moderates the relationship between rule tension and maladaptive behaviors.*

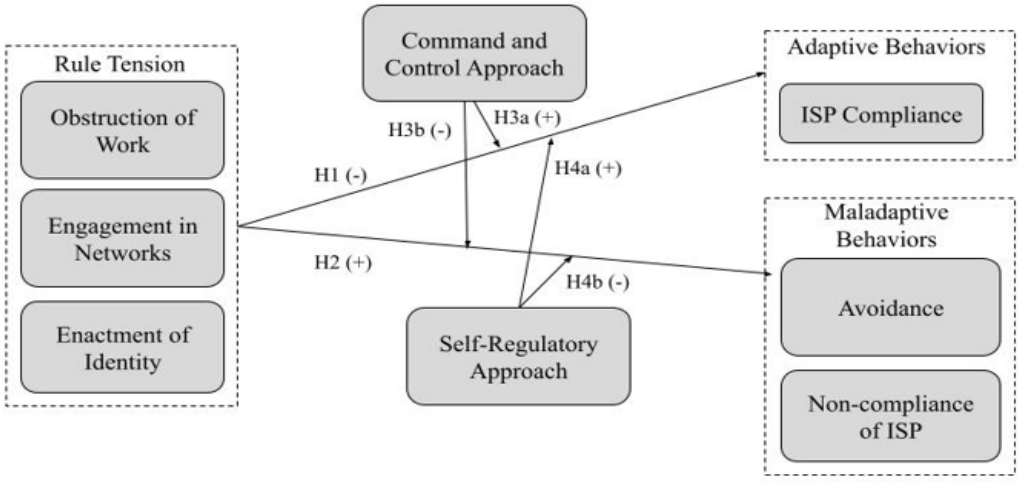


Figure 1: Research Model

Research Methods

A survey-based experiment administered to knowledge workers employed in companies with an information security policy was used to test the hypotheses. Rule tension is the independent variable of interest (Hannah & Robertson, 2015). Rule tension is theorized as a second-order construct comprised of (1) Obstruction of Work (e.g., "It is hard for me to comply with the information security policy when it makes it hard to perform work activities"), (2) Engagement in Networks (e.g., "The Information Security Policy prevents access to needed information from others"), and (3) Enactment of Identity (e.g., "I feel as if I lose credibility due to Information Security Policy and Policies"). Two moderating variables - command-and-control approach and self-regulatory approach were collected. Command-and-control approach (Yazdanmehr et al., 2020) is comprised of (1) detection of behavior (e.g., "It is easy for my organization to observe whether or not I follow the information security policy"), and (2) reaction to behavior (e.g., "If I am caught breaking the organization's policy, it hurts my pay or chances for promotion"). Self-regulatory approach (Yazdanmehr et al., 2020) is comprised of (1) legitimacy (e.g., "Organizations are most successful when employees follow the security policy") and (2) value congruence (e.g., "I find that my values and the values where I work are very similar.")

Two outcome variables were collected. Adaptive behaviors consist of ISP compliance intentions (Chen et al., 2021) (e.g., "I intend to comply with the requirements"). Maladaptive behaviors (Chen et al., 2021) consist of (1) Avoidance and (2) ISP noncompliance intentions. Avoidance is measured as a coping response to the stress of not being able to comply with the information security policy. At the same time finding other options (e.g., "If I were to purposely not comply with my organization's information security policy, my first instinct is to not worry about what would happen if I violated the security policy."). The variable non-compliance intentions were measured separately from compliance intentions (e.g., "I intend to NOT carry out my responsibilities prescribed in the requirements").

Results

474 participants were recruited via the platform Prolific, which utilized an online response panel. A large majority of respondents had achieved at least a college degree. The ages of respondents were generally equally divided between age groups (20-29, 30-39, etc.), and there was an almost equal distribution of management to non-management job responsibilities. Panel participants were removed when they indicated that they did not use a computer system for their job, that their organization did not have an information security policy (formal or informal) or answered any of the attention check questions incorrectly. The resulting data set consisted of 404 complete, valid responses. Instrument validity and reliability were examined using SmartPLS, version 4.1.0.0 (Ringle et al., 2022), summarized in Tables 1, 2, 3, and 4.

All model evaluation statistics exceeded their respective cutoffs (Hair et al. 2011). Indicator reliability was demonstrated because all items for each construct loaded at .765 or above. Internal consistency reliability was demonstrated because, for every construct, Cronbach's alpha was .843 or above, and composite reliability (rho_c) was .889 or above. Convergent validity was demonstrated because every construct's average variance extracted was .693 or above. Discriminant validity was demonstrated because the square root of the AVE of each latent construct is higher than the construct's highest correlation with any other latent construct (Table 2), and the heterotrait-monotrait ratio (HTMT) for each latent variable was .756 or below (Table 3), below the recommendation of .85 (Sarstedt et al. 2023). Furthermore, every indicator's loading on its latent variable is higher than its cross-loading with every other latent variable (Table 4).

Hypothesis results

The hypotheses were also tested using SmartPLS. Bootstrapping (5,000 subsamples) was used to determine the significance of path coefficients (two-tailed, $p < .05$). The results are summarized graphically in Figure

2. First, the appropriateness of second-order constructs was examined. The rule tension second-order construct was shown to be comprised of the latent variables obstruction of work (b = .460, p < .001), engagement in networks (b = .292, p < .001), and enactment of identity (b = .409, p < .001). The command-and-control approach second-order construct was shown to be comprised of detection of behavior (b = .625, p < .001) and reaction to behavior (b = .496, p < .001). The self-regulatory approach second-order construct was shown to be comprised of legitimacy (b = .716, p < .001) and value congruence (b = .455, p < .001). Hypothesis 1 was supported. The employees who perceive rule tension because of (a) obstruction of work, (b) engagement in networks, and (c) enactment of identity were less likely to indicate adaptive behaviors towards ISP, with those indicating higher rule tension indicating lower compliance intention (b = -.207, p < .001).

Table 1: Instrument Reliability

	Cronbach's alpha	Composite reliability (rho_c)	Average variance extracted (AVE)
Detection of behavior (CCA)	0.931	0.956	0.878
Compliance intention (CI)	0.931	0.956	0.878
Enactment of Identity (IN_EI)	0.916	0.947	0.857
Engagement in Networks (IN_EN)	0.843	0.905	0.761
Obstruction of work (IN_OW)	0.898	0.929	0.766
ISP Threats Avoidance (ISPTA)	0.904	0.938	0.835
Non-compliance intention (NCI)	0.928	0.955	0.875
Reaction to Behavior (RTB)	0.813	0.889	0.729
Legitimacy (SRA)	0.888	0.918	0.693
Value Congruence (VC)	0.925	0.947	0.817

Table 2: Correlation of Latent Variables (Square Root of AVE on Diagonals)

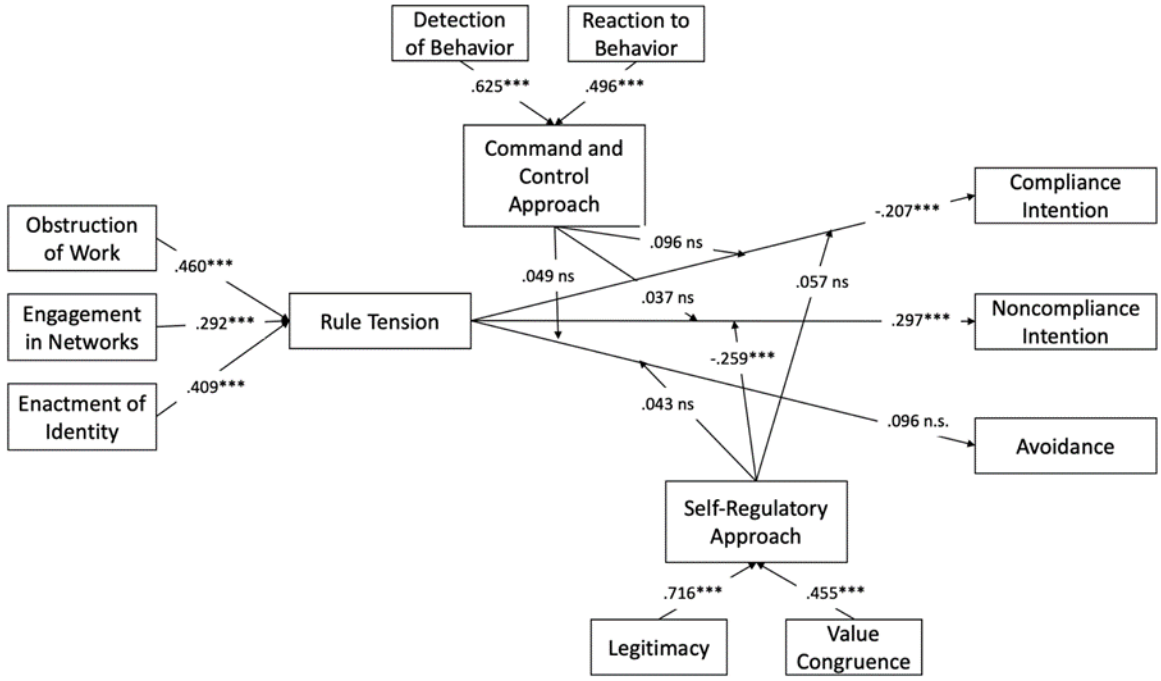
	CCA	CI	IN_EI	IN_EN	IN_OW	ISPTA	NCI	RTB	SRA	VC
CCA	0.937									
CI	0.227	0.937								
IN_EI	-0.003	-0.466	0.926							
IN_EN	-0.097	-0.263	0.514	0.872						
IN_OW	-0.072	-0.368	0.626	0.661	0.875					
ISPTA	-0.18	-0.124	0.155	0.104	0.074	0.914				
NCI	-0.086	-0.442	0.488	0.304	0.374	0.161	0.935			
RTB	0.588	0.264	-0.175	-0.1	-0.123	-0.12	-0.153	0.854		
SRA	0.328	0.682	-0.444	-0.252	-0.357	-0.165	-0.441	0.369	0.833	
VC	0.296	0.309	-0.14	-0.145	-0.154	-0.111	-0.171	0.193	0.43	0.904

Table 3: Construct Heterotrait-Monotrait Ratios (HTMT)

	CCA	CI	IN_EI	IN_EN	IN_OW	ISPTA	NCI	RTB	SRA
CI	0.243								

IN_EI	0.037	0.503							
IN_EN	0.108	0.292	0.578						
IN_OW	0.079	0.398	0.682	0.756					
ISPTA	0.194	0.119	0.158	0.113	0.074				
NCI	0.093	0.476	0.528	0.339	0.404	0.163			
RTB	0.676	0.305	0.203	0.12	0.142	0.133	0.177		
SRA	0.362	0.746	0.488	0.282	0.393	0.168	0.482	0.436	
VC	0.321	0.33	0.15	0.162	0.167	0.113	0.183	0.224	0.47

Hypothesis 2 was supported for noncompliance intention. The employees who perceive rule tension are more likely to exhibit maladaptive behaviors towards ISP, with those indicating higher rule tension indicating higher non-compliance intention (b = .297, p < .001), but no differences for avoidance (b = .096, p = .110).



* p<.05, ** p<.01, *** p<.001, ns Not Significant

Figure 2: Results

Hypothesis 3a was not supported. The command-and-control approach was not shown to significantly moderate the relationship between rule tension and ISP compliance (b = .096, p = .073).
Hypothesis 3b was not supported. The command-and-control approach was not shown to moderate the relationship between rule tension and the maladaptive behaviors of non-compliance intention (b = .037, p = .701) or avoidance (b = .049, p = .433).

Table 4: Item Loadings and Cross-Loadings

	CCA	CI	IN_EI	IN_EN	IN_OW	ISPTA	NCI	RTB	SRA	VC
CCA1	**0.94**	0.216	-0.006	-0.08	-0.073	-0.164	-0.091	0.545	0.323	0.258
CCA2	**0.928**	0.258	-0.042	-0.09	-0.064	-0.158	-0.094	0.565	0.326	0.287
CCA3	**0.944**	0.163	0.04	-0.102	-0.067	-0.185	-0.057	0.543	0.275	0.288
CI1	0.185	**0.929**	-0.432	-0.271	-0.352	-0.083	-0.429	0.227	0.624	0.287
CI2	0.234	**0.948**	-0.433	-0.237	-0.328	-0.152	-0.417	0.243	0.64	0.312
CI3	0.218	**0.935**	-0.444	-0.232	-0.355	-0.113	-0.398	0.272	0.653	0.269
IN_EI1	0.023	-0.375	**0.899**	0.479	0.546	0.118	0.384	-0.116	-0.387	-0.151
IN_EI2	-0.02	-0.43	**0.942**	0.497	0.563	0.166	0.444	-0.192	-0.416	-0.14
IN_EI3	-0.01	-0.484	**0.935**	0.452	0.628	0.146	0.522	-0.176	-0.429	-0.099
IN_EN1	-0.125	-0.238	0.457	**0.839**	0.584	0.119	0.288	-0.125	-0.267	-0.158
IN_EN2	-0.042	-0.152	0.349	**0.864**	0.507	0.055	0.193	-0.056	-0.11	-0.083
IN_EN3	-0.083	-0.285	0.523	**0.913**	0.629	0.093	0.303	-0.078	-0.267	-0.133
IN_OW1	-0.064	-0.304	0.556	0.594	**0.913**	0.041	0.341	-0.096	-0.31	-0.159
IN_OW2	-0.06	-0.266	0.472	0.573	**0.877**	0.077	0.271	-0.094	-0.275	-0.082
IN_OW3	-0.065	-0.258	0.414	0.603	**0.87**	0.062	0.224	-0.061	-0.223	-0.168
IN_OW4	-0.065	-0.445	0.725	0.546	**0.839**	0.08	0.457	-0.172	-0.428	-0.128
ISPTA1	-0.138	-0.03	0.069	0.076	0.027	**0.831**	0.081	-0.063	-0.059	-0.062
ISPTA2	-0.186	-0.096	0.15	0.075	0.053	**0.949**	0.145	-0.132	-0.154	-0.068
ISPTA3	-0.165	-0.174	0.176	0.124	0.104	**0.955**	0.186	-0.117	-0.199	-0.154
NCI1	-0.049	-0.376	0.455	0.285	0.349	0.11	**0.903**	-0.128	-0.396	-0.147
NCI2	-0.086	-0.434	0.462	0.279	0.354	0.177	**0.955**	-0.145	-0.419	-0.169
NCI3	-0.107	-0.43	0.451	0.29	0.347	0.163	**0.948**	-0.156	-0.422	-0.163
RTB1	0.521	0.139	-0.05	-0.055	-0.045	-0.08	-0.092	**0.857**	0.237	0.178

	CCA	CI	IN_EI	IN_EN	IN_OW	ISPTA	NCI	RTB	SRA	VC
RTB2	0.479	0.241	-0.186	-0.059	-0.13	-0.107	-0.15	**0.886**	0.319	0.09
RTB3	0.505	0.299	-0.215	-0.143	-0.142	-0.121	-0.151	**0.817**	0.393	0.227
SRA1	0.278	0.715	-0.476	-0.242	-0.358	-0.151	-0.468	0.327	**0.876**	0.374
SRA2	0.232	0.529	-0.35	-0.167	-0.264	-0.188	-0.352	0.293	**0.785**	0.273
SRA3	0.259	0.525	-0.388	-0.226	-0.276	-0.158	-0.338	0.385	**0.822**	0.376
SRA4	0.299	0.628	-0.404	-0.236	-0.341	-0.128	-0.412	0.299	**0.906**	0.411
SRA5	0.298	0.421	-0.213	-0.169	-0.237	-0.061	-0.249	0.23	**0.765**	0.345
VC1	0.276	0.305	-0.167	-0.169	-0.14	-0.113	-0.168	0.197	0.425	**0.917**
VC2	0.257	0.286	-0.101	-0.095	-0.165	-0.102	-0.148	0.163	0.391	**0.896**
VC3	0.253	0.304	-0.162	-0.118	-0.166	-0.096	-0.172	0.154	0.404	**0.941**
VC4	0.289	0.214	-0.067	-0.141	-0.079	-0.09	-0.126	0.186	0.327	**0.861**

Hypothesis 4a was not supported. The self-regulatory approach was not shown to moderate the relationship between rule tension and the adaptive behavior of ISP compliance intention (b = .057, p = .558). Hypothesis 4b was partially supported. The self-regulatory approach negatively moderates the relationship between rule tension and the maladaptive behavior of non-compliance intention (b = -.259, p < .001), but not avoidance (b = .043, p = .354). In addition to testing the hypothesized moderation effects for command-and-control and self-regulatory approach, the PLS models also included direct effects of those on the adaptive and maladaptive behaviors. The command-and-control approach had no significant direct path coefficient with any of the dependent variables (|b| <= .112, p >= .056). The self-regulatory approach had significant path coefficients with compliance intention (b = .503, p < .001) and non-compliance intention (b = -.185, p = .003), but not with avoidance (b = -.107, p = .099).

Finally, PLS also computes the significance of indirect effects, meaning we can offer further insights about how the components of each second-order construct each had a share of the impact on the DVs. Impacting compliance intention, significant indirect effects were shown for enactment of identity through rule tension (b = -.085, p = .001), engagement of networks through rule tension (b = -.061, p < .001), obstruction of work through rule tension (b = -.095, p < .001), legitimacy through self-regulatory approach (b = .360, p < .001), and value congruence through self-regulatory approach (b = .229, p < .001). Impacting noncompliance intention, significant indirect effects were shown for enactment of identity through rule tension (b = .122, p < .001), engagement in networks through rule tension (b = .087, p < .001), obstruction of work through rule tension (b = .136, p < .001), legitimacy through self-regulatory approach (b = -.133, p = .002), and value congruence through self-regulatory approach (b = -.084, p = .004). There were no significant indirect effects for avoidance.

Discussion

This study aims to shed light on the effect of rule tension on employee's information security behavior. Results indicate that rule tension negatively influences ISP compliance, which is an adaptive behavior. Among maladaptive behaviors, rule tension has a positive relationship with non-compliance but does not significantly affect avoidance. Contrary to expectations, we found no significant moderating influence of the command-and-control approach on the relationship between rule tension and information security behavior. This finding is consistent with previous studies that have questioned the command-and-control approach's relevance in the self-regulatory approach's presence (Ifinedo, 2014; Li et al., 2014).

The results indicate that when employees face tensions between ISP requirements and the ability to complete work tasks, the threat of sanctions or rewards from management has no bearing on whether to break the ISP. However, employees may be more concerned with sanctions for not completing work as opposed to complying with ISPs when tension persists. This could be an important avenue to investigate further for ISP compliance. On the other hand, the self-regulatory approach was found to diminish the effect of rule tension on ISP non-compliance while not showing any moderating effect on other outcome variables. This interesting result supports the assertion that compliance and non-compliance are not exactly opposite concepts (Chen et al., 2022; Karjalainen et al., 2019). These results also suggest that when faced with rule tensions when completing work tasks, intrinsically motivated individuals seek to minimize maladaptive behaviors for the organization's benefit.

The results of the study have implications for theory in the following ways. To begin with, this study is the first to introduce the concept of rule tension to the information security literature, thus paving the way for future research. Taking the theoretical perspective of rule-following, rule tension is a source of security-related stress that reduces adaptive behavior and promotes maladaptive behaviors. Future studies should explore the factors that could potentially reduce the impact of rule tension on employee rule-following behavior. In addition, our study identifies three types of tensions that employees can face while following information security rules: obstruction to their work, engagement in external and internal networks, and identity enactment. Future research could delve deeper into these types of rule tension and how these impact employee behaviors.

Second, this study proposes a model that accounts for adaptive (compliance) and maladaptive (non-compliance and avoidance) behaviors in the context of behavioral information security research, thus propositioning dual coping outcomes. Our results demonstrate that the influence of rule tension on the outcome variables – compliance, non-compliance, and avoidance are not the same. Thus, by taking a more holistic approach that has received less attention in information security research, we address a call by Chen et al. (2022) to expand the understanding of security-related behaviors further and study their differences. While there is a plethora of research on ISP compliance and violations in isolation, our research reiterates that compliance/non-compliance outcomes are not opposites of each other but distinct constructs, and there is still a need for future research to consider the adaptive and maladaptive rewards simultaneously and to understand the tipping point. Additionally, our study highlights the need for future research to understand the antecedents of employee avoidance behavior.

Further, our study proposes that the relationship between rule tension and rule-following (adaptive or maladaptive) behaviors can be moderated by two approaches: (1) command-and-control and (2) self-regulatory. The greater IS literature rarely investigates the command-and-control and self-regulatory approaches as relationship enhancers. Yazdanmehr et al. (2020) reviewed the two constructs as antecedents to ISP violations, finding the importance of social influence in motivating ISP compliance between the two strategies. The results of our study show that while the command-and-control approach did not have any

moderating influence on the relationship between rule tension and employee behavior, the self-regulatory approach helped to alleviate the influence of rule tension on non-compliance. Thus, our findings add to the literature a more nuanced connection between these two approaches than previously understood and highlight the importance of an intrinsically motivated self-regulatory approach over an extrinsically motivated command-and-control approach. Future studies could also investigate other factors that may help moderate or mediate the influence of rule tension on employee behaviors.

Finally, the study also offers relevant practical insights. Many users consider security-related tasks a barrier to getting their work done, engaging with important others within and outside the organization, or enacting their identities. Awareness of these rule tensions will help managers and the IS function design information security policies and procedures better to reduce rule tension for employees. Additionally, it is important to review information security policies frequently and revise unnecessary ones that may be sources of rule tension.

The study's results indicate that the self-regulatory governance approach is effective in reducing ISP non-compliance due to rule tension. Managers should, therefore, consider leveraging this approach and investing in resources and training to intrinsically motivate their employees. Managers may also benefit from promoting open communication with their employees and getting feedback about the information security policies and procedures, especially given the rapidly changing threat landscape.

Limitations

There are some limitations in the study that create opportunities for future research. First, the data collection for our study was cross-sectional. Future studies could use longitudinal data to understand this context's relationships better. Second, the study is based on self-reported measures of the information security behavior of the participants. While this is in line with existing information security literature

(Bulgurcu et al., 2010; Chen et al., 2022), future studies could extend the understanding of rule-following behavior by measuring the actual information security behavior of employees or by triangulating the self-reported behaviors with input from the supervisors. Finally, we focused on rule tension but did not account for other potential sources of stress. Future studies could look at rule tension in the presence of other stressors.

Conclusion

In this study, we examined the influence of rule tension on an employee's rule-following behavior toward information security policy. When faced with security-related rule tension, employees are less likely to exhibit adaptive behavior and more likely to exhibit maladaptive behavior. In the study, command-and-control did not moderate the relationship between rule tension and information security behavior. On the other hand, our results indicated that the self-regulatory approach helps by weakening the effect of rule tension on non-compliance towards information security policy but had no such effect on ISP compliance or avoidance outcomes. The study's practical implication highlights the need to review security policies frequently and revise unnecessary ones causing security-related rule tension. Additionally, it is an impetus to promote the intrinsically motivated self-regulatory governance approach.

References

Ament, C., & Haag, S. (2016). Security-related stress–a neglected construct in information systems stress literature.

Ayyagari, R., Grover, V., & Purvis, R. (2011). Technostress: Technological antecedents and implications. *MIS quarterly*, 831-858.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), 151-164.

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

Calic, D., Pattinson, M. R., Parsons, K., Butavicius, M. A., & McCormac, A. (2016). Naïve and Accidental Behaviours that Compromise Information Security: What the Experts Think. HAISA,

Chen, X., Wu, D., Chen, L., & Teng, J. K. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management*, *55*(8), 1049-1060.

Chen, Y., Galletta, D. F., Lowry, P. B., Luo, X., Moody, G. D., & Willison, R. (2021). Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model. *Information Systems Research*, *32*(3), 1043-1065.

Chen, Y., Luo, X. R., & Li, H. (2022). Beyond adaptive security coping behaviors: Theory and empirical evidence. *Information & Management*, *59*(2), 103575.

Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS Quarterly*, *43*(2).

Cram, W. A., Proudfoot, J. G., & John, D. A. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems*, *26*(6), 605-641.

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643-658.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective: JMIS JMIS. *Journal of management information systems*, *31*(2), 285.

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

D'Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, *29*(1), 43-69.

D'Arcy, J., & Teh, P.-L. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management*, *56*(7), 103151.

Gooty, J., Gavin, M. B., Ashkanasy, N. M., & Thomas, J. S. (2014). The wisdom of letting go and performance: The moderating role of emotional intelligence and discrete emotions. *Journal of occupational and organizational psychology*, *87*(2), 392-413.

Hannah, D. R., & Robertson, K. (2015). Why and how do employees break and bend confidential information protection rules? *Journal of Management Studies*, *52*(3), 381-413.

Hedström, K., Karlsson, F., & Kolkowska, E. (2013). Social action theory for understanding information security non-compliance in hospitals: The importance of user rationale. *Information Management & Computer Security*, *21*(4), 266-287.

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems*, *20*(4), 373-384.

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management*, *49*(2), 99.

Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior*, *81*, 282-293.

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

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: influences on information security policy violations. *European Journal of Information Systems*, *25*(3), 231-251.

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

Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security*, *33*, 3-11.

Kranz, J., & Haeussinger, F. (2014). Why deterrence is not enough: The role of endogenous motivations on employees' information security behavior.

Li, H., Sarathy, R., Zhang, J., & Luo, X. (2014). Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. *Information Systems Journal*, *24*(6), 479-502.

Liu, Y., Yu, C., Sheng, J., & Zhang, T. (2018). Self-collision Avoidance Trajectory Planning and Robust Control of a Dual-arm Space Robot: IJCAS IJCAS. *International Journal of Control, Automation, and Systems*, *16*(6), 2896-2905.

Malhotra, Y., Galletta, D. F., & Kirsch, L. J. (2008). How endogenous motivations influence user intentions: Beyond the dichotomy of extrinsic and intrinsic user motivations. *Journal of Management Information Systems*, *25*(1), 267-300.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS quarterly*, *42*(1), 285.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, *18*(2), 126-139.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013). An analysis of information security vulnerabilities at three Australian government organisations. *Proceedings of the European Information Security Multi-Conference, EISMC 2013*, 34-44.

Posey, C., Raja, U., Crossler, R. E., & Burns, A. J. (2017). Taking stock of organisations' protection of privacy: categorising and assessing threats to personally identifiable information in the USA. *European Journal of Information Systems*, *26*(6), 585-604.

Ringle, C. M., Wende, S., & Becker, J.-M. (2022). SmartPLS 4. Oststeinbek: SmartPLS. *Retrieved March*, *13*, 2023.

Rodell, J. B., & Judge, T. A. (2009). Can "good" stressors spark "bad" behaviors? The mediating role of emotions in links of challenge and hindrance stressors with citizenship and counterproductive behaviors. *Journal of applied psychology*, *94*(6), 1438.

Siponen, M., & Iivari, J. (2006). Six Design Theories for IS Security Policies and Guidelines 1. *Journal of the Association for Information Systems*, *7*(7), 445-472.

Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, *48*(7), 296.

Splunk. (2023). *The State of Security 2023*. https://www.splunk.com/en_us/campaigns/state-of-security.html

Tyler, T. R. (2006). Psychological perspectives on legitimacy and legitimation. *Annu. Rev. Psychol.*, *57*, 375-400.

Tyler, T. R., & Blader, S. L. (2005). Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. *Academy of Management Journal*, *48*(6), 1143-1158.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, *18*(2), 101-105.

Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, *92*, 36-46.

Yazdanmehr, A., Wang, J., & Yang, Z. (2020). Peers matter: The moderating role of social influence on information security policy compliance. *Information Systems Journal*.