

DOI: https://doi.org/10.48009/3_iis_2026_146

When policies meet work: Rule tension and employee responses to information security demands

Dr. Darin C. Hodges, *Appalachian State University*, hodgesdc@appstate.edu

Dr. Russell Haines, *Appalachian State University*, hainesrp@appstate.edu

Abstract

Employees frequently encounter situations in which information security policies (ISPs) conflict with the practical demands of their work, creating tensions that shape their security-related decisions. This study examines how different forms of rule tension influence adaptive (compliance) and maladaptive (noncompliance and avoidance) behaviors toward ISPs. Drawing on a rule-following perspective, we conceptualize rule tension as a multidimensional construct encompassing obstruction of work, constraints on network engagement, and conflicts with identity enactment. Using a scenario-based design and partial least squares analysis, we find that these dimensions exert distinct behavioral effects. Identity-related tension has the strongest and most consistent effects, reducing compliance while increasing noncompliance and avoidance. In contrast, work-related obstruction increases maladaptive behaviors without significantly reducing compliance intention, suggesting that employees may intend to comply while engaging in workarounds. We also examine governance approaches and find that self-regulatory perceptions have significant direct effects across all outcomes, while command-and-control shows no significant impact. These findings contribute by demonstrating that rule tension is not uniform, integrating adaptive and maladaptive behaviors within a single framework, and reconceptualizing governance approaches as motivational climates rather than situational moderators. The results highlight the importance of aligning ISPs with employees' work practices, social dynamics, and identities.

Keywords: ISP compliance; information security; rule tension; adaptive security behavior; maladaptive security behavior; avoidance

Introduction

Cybersecurity incidents frequently reflect the tension employees face between following security policies and breaking them to accomplish their work. Recent examples include a phishing campaign that leveraged urgent, policy-themed messages to pressure employees into complying with illegitimate requests, leading to widespread credential compromise (Intelligence, 2026). In a separate incident, a misconfigured API did not enforce fundamental data and access control policies and exposed sensitive employee data (AnuPriya, 2025). The growing integration of AI into organizational workflows has introduced new risks, as employees rely on automated guidance that may conflict with established security practices, as seen in a case where an employee relied on guidance from an AI agent about an engineering problem, leading to significant internal data exposure (Down, 2026). These incidents suggest that security failures are often less about malicious intent and more about how employees navigate competing demands in real-world work settings.

Information security policies (ISPs) are designed to guide employee behavior and reduce organizational risk; however, they are enacted within complex work environments that prioritize efficiency, collaboration, and responsiveness (Bulgurcu et al., 2010). When policies disrupt work processes, limit engagement with colleagues, or constrain how employees enact their professional roles, employees may experience rule tension, or psychological strain arising from conflicts between organizational rules and situational demands (Hannah & Robertson, 2015). In response, employees may comply with policies, engage in noncompliance, or avoid security-related decisions altogether, reflecting both adaptive and maladaptive behavioral patterns (Ali et al., 2021; Chen et al., 2022).

We take as a starting point the notion that rule tension manifests in multiple ways depending on how policies intersect with work. Specifically, employees may perceive policies as obstructing their ability to complete tasks, limiting engagement in professional networks, or constraining identity enactment within their roles. The focus of this paper is to examine how these distinct forms of rule tension influence adaptive and maladaptive behaviors toward ISPs. We further consider how organizational governance approaches, specifically command-and-control and self-regulatory strategies, shape employee responses in these situations.

By examining employee behavior through the lens of rule tension, this study seeks to provide a more nuanced understanding of how individuals make security-related decisions when policies come into conflict with the practical realities of their work. We conceptualize rule tension as a multidimensional construct and examine how its distinct forms shape adaptive and maladaptive security behaviors.

Theoretical Background and Literature Review

For employees who work in environments where information security policies (ISPs) intersect with complex and dynamic work demands, ISPs aim to protect organizational assets and information, but they often impose constraints that conflict with employees' task goals, collaboration needs, and professional identities. Research indicates that decisions not to follow ISPs often arise from employees' inability to complete work tasks (Hodges et al., 2024). These tensions are real; they occur in concrete situations where employees must decide how to act under competing pressures.

Rule tension refers to the subjective experience when organizational rules interfere with employees' ability to perform their work effectively (Hannah & Robertson, 2015). Rules are "explicit or implicit norms, regulations, and expectations that regulate the behavior of individuals and interaction among them." Importantly, rule tension is not monolithic – it manifests differently depending on the situation employees face. In information security, rule tension is especially relevant because ISPs often create friction in daily workflows (Bulgurcu et al., 2010; D'Arcy & Lowry, 2019). Security-related stressors such as work impediments, access restrictions, and identity threats can trigger both adaptive and maladaptive coping responses (Ayyagari et al., 2011; D'Arcy et al., 2014; Hwang & Cha, 2018).

Instead of viewing rule tension as a generalized psychological state, this study adopts a **scenario-based perspective** to examine how employees navigate ISP decisions across distinct contexts. This approach responds to recent ISP literature calling for more holistic and nuanced frameworks (Chen et al., 2022; Karjalainen et al., 2019) that account for both the type of tension experienced and the behaviors elicited. Thus, adaptive and maladaptive responses are best understood through discrete, contextually grounded scenarios, rather than a single motivational model.

In this study, rule tension is conceptualized as a second-order construct comprising four theoretically distinct situational demands that employees encounter in the course of everyday work. Obstruction of work occurs when ISP requirements directly impede the completion of primary work tasks. Engagement in personal networks, both internal and external, involves situations in which intra- or inter-organizational social relationships and informal norms create pressure to deviate from stated ISP requirements. The enactment of identity creates situations in which employees' professional or personal self-concepts conflict with ISP demands.

Each construct is theorized to generate a qualitatively different form of rule tension, which in turn shapes the probability of adaptive versus maladaptive behavioral responses. For this study, we follow a scenario-based design that strengthens theoretical understanding by prompting these forms of tension in real-world situations that employees can face daily.

Adaptive and Maladaptive Coping Responses

Information security behavior can be understood through the lens of coping theory (D'Arcy et al., 2014). Adaptive behaviors, such as ISP compliance, reflect problem-focused coping aimed at reducing security threats. Maladaptive behaviors, such as avoidance and non-compliance, reflect emotion-focused coping that reduces discomfort but increases organizational risk (Li & Huang, 2020; Liang et al., 2019; Yazdanmehr et al., 2023). Research has shown that work impediments can be useful in determining whether an individual will choose to break rules and rationalize that behavior to relieve stressors the rules create (D'Arcy & Lowry, 2019; Hannah & Robertson, 2015).

According to Security-Related Stress (SRS) theory (D'Arcy et al., 2014), employees facing work-obstructive rule tension are more likely to use neutralization strategies, rationalizing that policies are impractical or burdensome to justify non-compliance. Myyry et al. (2009) and Guo et al. (2011) show that identity-related tensions similarly predict non-compliance when workplace rules reduce credibility or conflict with professional identity. Yazdanmehr et al. (2020) highlights the influence of peers and social identity on security-related decisions. Together, these findings suggest that employees are more likely to reject compliance norms and seek workarounds as coping mechanisms, either to solve ISP-related problems or to justify non-compliance.

The four scenario-specific constructs developed in this study each correspond to a distinct coping pathway:

- **Obstruction of work** produces primarily **task-instrumental** rule tension, where the perceived cost of compliance is immediate, tangible, and directly tied to performance outcomes, making maladaptive workaround behaviors particularly likely.
- **External network engagement** produces **relationally instrumental** rule tension, where competing obligations to external professional relationships create pressure toward partially compliant or avoidant behaviors.
- **Internal network engagement** produces **socially normative** rule tension, in which descriptive peer norms within the workgroup may normalize deviations from formal ISP requirements.
- **Identity enactment** produces **intrinsically motivational** rule tension, arising not from external task or relational pressure but from an internal conflict between the self-concept and the behavioral demands of the policy, potentially eliciting both principled non-compliance and adaptive advocacy behavior.

Governance Approaches as Motivational Climate

Information security governance strategies shape how employees interpret and respond to ISP requirements across all four scenario-based constructs. Two dominant approaches are widely studied:

- **Command-and-Control:** Based on deterrence theory, emphasizing monitoring, sanctions, and compliance enforcement (Johnston et al., 2016; Siponen & Iivari, 2006).
- **Self-Regulatory:** Based on internalization, value congruence, and legitimacy, emphasizing intrinsic motivation to comply (Son, 2011; Tyler & Blader, 2005; Yazdanmehr & Wang, 2016).

These two governance approaches are typically applied within each scenario-specific pathway. However, rather than functioning merely as moderators of the rule tension–behavior relationship, prior research on legitimacy and intrinsic motivation suggests that governance approaches shape how employees interpret ISPs’ legitimacy and demands across situational contexts.

Hypotheses Development

Obstruction of Work: When ISPs impede task completion, employees experience frustration and resource depletion, increasing the appeal of shortcuts and avoidance strategies (Ayyagari et al., 2011; D’Arcy & Lowry, 2019).

- **H1a:** Obstruction of work will be negatively associated with compliance intention.
- **H1b:** Obstruction of work will be positively associated with non-compliance intention.
- **H1c:** Obstruction of work will be positively associated with avoidance.

Engagement in Networks: When ISPs restrict collaboration or information sharing, employees experience network-related tension that undermines compliance and encourages workarounds (Kolkowska & Dhillon, 2013; Karjalainen et al., 2019).

- **H2a:** Engagement-in-networks tension will be negatively associated with compliance intention.
- **H2b:** Engagement-in-networks tension will be positively associated with non-compliance intention.
- **H2c:** Engagement-in-networks tension will be positively associated with avoidance.

Enactment of Identity: When ISPs threaten credibility, autonomy, or professional identity, employees experience identity-related tension that strongly pushes them toward maladaptive coping (Hedström et al., 2011; Myyry et al., 2009).

- **H3a:** Identity-related tension will be negatively associated with compliance intention.
- **H3b:** Identity-related tension will be positively associated with non-compliance intention.
- **H3c:** Identity-related tension will be positively associated with avoidance.

Governance Approaches as Direct Antecedents

Self-Regulatory Governance: Employees who perceive ISP rules as legitimate and aligned with their values are more likely to internalize compliance and reject maladaptive coping (Tyler, 2006; Son, 2011).

- **H4a:** Self-regulatory perceptions will be positively associated with compliance intention.
- **H4b:** Self-regulatory perceptions will be negatively associated with non-compliance intention.
- **H4c:** Self-regulatory perceptions will be negatively associated with avoidance.

Command-and-Control Governance: Although deterrence may influence compliance in some contexts, its effects are inconsistent in knowledge-work environments where employees face ambiguous, high-pressure decisions (Hovav & D’Arcy, 2012; Liu et al., 2018).

- **H5a:** Command-and-control perceptions will be positively associated with compliance intention.
- **H5b:** Command-and-control perceptions will be negatively associated with non-compliance intention.
- **H5c:** Command-and-control perceptions will be negatively associated with avoidance.

Figure 1 graphically summarizes the research model.

Figure 1: Research Model

Methodology

This study employed a scenario-based experimental design to investigate how employees respond to information security policy (ISP) decisions in distinct workplace contexts. The scenario-based approach enables the systematic manipulation of rule tension dimensions in realistic, work-related situations while minimizing confounding variables (Aguinis & Bradley, 2014; Ragu-Nathan et al., 2008). Scenarios were written, edited, and authenticated through multiple iterations and academic peer feedback. Additionally, scenarios were presented and vetted with working individuals who could have previously encountered, or might in the future encounter, a situation in which the scenario could arise, to ensure authenticity. Rule tension was operationalized through four scenario conditions, with each scenario designed to simulate one theoretically distinct variable of rule tension encountered in organizational settings:

Obstruction of Work Scenario – Participants read about a situation in which strict ISP requirements (e.g., multi-step approval processes and encryption mandates) significantly delay time-sensitive deliverables and reduce work efficiency.

Engagement in Internal Networks Scenario – Participants encounter a situation in which ISP rules prohibit the easy sharing of non-sensitive project files with internal team members, hindering collaboration.

Engagement in External Networks Scenario – Participants face restrictions on sharing information or using collaborative tools with external partners and clients, limiting networking and innovation opportunities.

Enactment of Identity Scenario – Participants read about policies that conflict with their professional identity or personal values (e.g., overly restrictive monitoring that makes them feel distrusted or undermines their autonomy as knowledgeable professionals).

Participants, Procedures and Measures

Participants were recruited via a Prolific panel, with the prequalification that they needed to use a computer for work and that their firm had a security policy. Out of the initial 474 recruited participants, participants were removed from the panel when they indicated: (1) that they did not use a computer system for their job, (2) that their organization did not have a security policy, or (3) answered any of the attention check questions incorrectly. This left 404 complete, valid responses in the final data set.

Data collection began with participants completing demographic questions and governance orientation measures. Next, participants were randomly assigned to one of the four scenario conditions and instructed to read the scenario thoroughly. Afterward, they completed behavioral intention items and manipulation-check measures for the scenario. This order ensured that governance orientation was assessed prior to scenario exposure, reducing the risk of contamination between moderator and manipulation variables.

Antecedents: Two governance antecedents were included and adapted from Yazdanmehr et al. (2023).

- *Command-and-Control Approach* – capturing perceptions of monitoring, sanctions, and enforcement-based compliance pressure
- *Self-Regulatory Approach* – capturing perceptions of policy legitimacy, value congruence, and intrinsic motivation to comply

Dependent Variables: Three behavioral intention outcomes were assessed:

- *ISP Compliance Intentions* – representing adaptive behavioral responses (Chen et al., 2021)
- *ISP Non-Compliance Intentions* – representing maladaptive behavioral responses (Chen et al., 2021)
- *Avoidance Intentions* – representing a second form of maladaptive behavioral response (Chen et al., 2021)

All scales used 7-point Likert-type response formats. Manipulation checks confirmed that each scenario successfully induced the intended type of rule tension before proceeding to substantive analysis.

Results

Data analysis employed Partial Least Squares Structural Equation Modeling (PLS-SEM) to test the relationships between latent constructs. Supplementary analyses included ANOVA and MANOVA to examine main effects across the four scenario conditions, as well as moderated regression analyses to assess the interactive effects of governance orientation on behavioral intentions in each scenario.

Instrument Validity and Reliability

We used SmartPLS, version 4.1.0.0 (Ringle et al., 2022) for hypothesis testing and to evaluate the validity and reliability of the questionnaire instruments. The model included all scenarios, with dummy variables to control for scenario differences. The relevant statistics are summarized in Tables 1, 2, 3, and 4 below. For all statistics, the criteria recommended by Hair et al. (2011) was used to assess validity and reliability. Table 1 shows that Cronbach's alpha was .744 or above for all constructs; furthermore, composite reliability for all constructs was .813 or above, which exceeds the recommended values for exploratory (.6) and more

mature research (.7). Table 1 also shows that average variance extracted (AVE) was .660 or above for all latent variables, exceeding the .5 cutoff, which indicates convergent validity.

Table 2 shows that the square root of AVE is higher for all constructs than the highest correlation of each construct with any other latent variable. Table 3 shows that each item loads higher on its own latent variable than any other latent variable. Heterotrait-monotrait ratios (HTMT) are within a .85 conservative cutoff (Sarstedt et al., 2023). Together, these indicate discriminant validity.

Table 1. Reliability of Instruments

	Cronbach's alpha	Composite reliability (rho_c)	Average variance extracted (AVE)
Detection of behavior (CCA)	0.931	0.956	0.878
Enactment of Identity (SEI)	0.921	0.950	0.864
Engagement in Networks (SEN)	0.833	0.895	0.743
Obstruction of work (OW)	0.835	0.886	0.660
Reaction to Behavior (RTB)	0.813	0.889	0.729
Compliance intention (SCI)	0.946	0.965	0.903
Non-compliance intention (SNCI)	0.977	0.985	0.955
Legitimacy (SRA)	0.888	0.918	0.693
ISP Threats Avoidance (STA)	0.876	0.924	0.803
Value Congruence (VC)	0.925	0.947	0.817

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

	CCA	RTB	SCI	SEI	SEN	SNCI	SOW	SRA	STA	VC
CCA	0.937									
RTB	0.588	0.854								
SCI	0.140	0.213	0.950							
SEI	0.047	0.003	-0.277	0.929						
SEN	-0.142	-0.045	-0.029	0.474	0.862					
SNCI	-0.126	-0.191	-0.637	0.351	0.113	0.977				
SOW	-0.139	-0.104	-0.189	0.605	0.665	0.304	0.813			
SRA	0.328	0.369	0.447	-0.145	-0.035	-0.385	-0.124	0.833		
STA	-0.143	-0.168	-0.560	0.323	0.086	0.792	0.262	-0.400	0.896	
VC	0.296	0.193	0.142	0.008	-0.163	-0.106	-0.106	0.430	-0.179	0.904

Table 3: Item Loadings and Cross Loadings

	CCA	RTB	SRA	SCI	SEI	SEN	SNCI	SOW	STA	VC
CCA1	0.940	0.545	0.323	0.138	0.043	-0.16	-0.126	-0.144	-0.143	0.258
CCA2	0.928	0.565	0.326	0.161	0.049	-0.089	-0.158	-0.130	-0.166	0.287
CCA3	0.944	0.543	0.275	0.093	0.041	-0.151	-0.069	-0.117	-0.092	0.288
RTB1	0.521	0.857	0.237	0.128	0.087	-0.021	-0.090	-0.033	-0.126	0.178
RTB2	0.479	0.886	0.319	0.179	-0.049	-0.028	-0.198	-0.099	-0.139	0.090
RTB3	0.505	0.817	0.393	0.241	-0.032	-0.067	-0.203	-0.135	-0.166	0.227
SRA1	0.278	0.327	0.876	0.457	-0.139	-0.015	-0.391	-0.086	-0.415	0.374
SRA2	0.232	0.293	0.785	0.354	-0.126	0.023	-0.316	-0.084	-0.330	0.273
SRA3	0.259	0.385	0.822	0.365	-0.118	-0.050	-0.313	-0.145	-0.319	0.376
SRA4	0.299	0.299	0.906	0.405	-0.130	-0.028	-0.356	-0.091	-0.373	0.411
SRA5	0.298	0.230	0.765	0.265	-0.086	-0.074	-0.214	-0.112	-0.216	0.345
SCI1	0.109	0.196	0.412	0.934	-0.275	-0.029	-0.609	-0.165	-0.540	0.130
SCI2	0.123	0.198	0.396	0.956	-0.275	-0.038	-0.614	-0.202	-0.511	0.123
SCI3	0.164	0.213	0.463	0.961	-0.243	-0.016	-0.595	-0.171	-0.545	0.152
SEI1	0.033	0.005	-0.148	-0.247	0.916	0.437	0.307	0.545	0.283	0.003
SEI2	0.048	-0.008	-0.145	-0.265	0.930	0.429	0.351	0.563	0.307	-0.002
SEI3	0.049	0.011	-0.111	-0.260	0.941	0.457	0.319	0.577	0.310	0.020
SEN1	-0.121	-0.112	-0.003	-0.062	0.427	0.717	0.175	0.671	0.182	-0.140
SEN2	-0.116	-0.005	-0.011	0.016	0.326	0.909	0.024	0.517	0.019	-0.178
SEN3	-0.136	-0.037	-0.057	-0.042	0.491	0.942	0.128	0.615	0.078	-0.122
SNCI1	-0.126	-0.205	-0.376	-0.646	0.346	0.102	0.983	0.286	0.778	-0.106
SNCI2	-0.114	-0.168	-0.369	-0.598	0.325	0.109	0.971	0.301	0.769	-0.096
SNCI3	-0.129	-0.187	-0.384	-0.623	0.359	0.120	0.979	0.304	0.777	-0.107
SOW1	-0.126	-0.085	-0.033	-0.080	0.424	0.586	0.201	0.835	0.187	-0.094
SOW2	-0.041	-0.088	-0.118	-0.222	0.470	0.468	0.294	0.827	0.263	-0.001
SOW3	-0.153	-0.068	-0.015	-0.057	0.365	0.547	0.140	0.768	0.151	-0.155
SOW4	-0.149	-0.090	-0.174	-0.192	0.625	0.579	0.292	0.818	0.221	-0.123
STA1	-0.154	-0.088	-0.273	-0.387	0.273	0.113	0.562	0.238	0.825	-0.205
STA2	-0.111	-0.169	-0.361	-0.538	0.312	0.094	0.746	0.257	0.934	-0.131
STA3	-0.124	-0.185	-0.430	-0.565	0.285	0.032	0.802	0.213	0.925	-0.153
VC1	0.276	0.197	0.425	0.169	-0.044	-0.189	-0.123	-0.126	-0.172	0.917
VC2	0.257	0.163	0.391	0.109	0.027	-0.126	-0.09	-0.081	-0.176	0.896
VC3	0.253	0.153	0.404	0.144	-0.007	-0.138	-0.102	-0.106	-0.164	0.941
VC4	0.290	0.186	0.327	0.087	0.059	-0.136	-0.064	-0.067	-0.135	0.861

Table 4: Construct Heterotrait-Monotrait Ratios (HTMT)

	CCA	RTB	SCI	SEI	SEN	SNCI	SOW	SRA	STA
RTB	0.676								
SCI	0.148	0.244							
SEI	0.051	0.077	0.297						
SEN	0.163	0.073	0.052	0.547					
SNCI	0.132	0.215	0.663	0.369	0.139				
SOW	0.163	0.126	0.189	0.656	0.835	0.314			
SRA	0.362	0.436	0.484	0.160	0.054	0.411	0.133		
STA	0.160	0.195	0.609	0.360	0.138	0.850	0.296	0.446	
VC	0.321	0.224	0.150	0.044	0.193	0.110	0.139	0.470	0.202

Descriptive Statistics

Descriptive statistics for each construct by scenario are shown in Table 5, with significant differences between scenarios noted. With respect to obstruction of work, respondents who viewed scenario 4 (sharing health-related data with an outside firm) perceived the information security policy to be significantly more obstructive to work than respondents who viewed scenarios 1 (copying data to another device), 2 (sharing customer purchase histories with an internal colleague), or 3 (sharing customer purchase histories with another supply chain member). With respect to engagement in networks, ISPs were perceived to be significantly more inhibitive of building networks for respondents who viewed scenarios 2, 3, and 4 than for those who viewed scenario 1, and were perceived to be significantly more inhibitive for scenario 4 than for scenario 2. With respect to the enactment of identity, ISPs were perceived to be significantly more inhibiting of the building of personal capital for respondents who viewed scenario 4 than for those who viewed scenarios 1 or 2. There were no significant differences among respondents viewing each scenario with respect to ISP compliance, avoidance, or ISP non-compliance ($p \leq .068$).

Table 5: Means and (standard deviations) by Scenario

	Scen 1	Scen 2	Scen 3	Scen 4	ANOVA p-value	Tukey post-test results ($p < .05$)
n	102	101	101	100		
SO W	4.00 (1.33)	4.01 (1.24)	3.85 (1.46)	4.61 (1.11)	<.001	4 > 1, 4 > 2, 4 > 3
SEN	4.02 (1.48)	4.63 (1.50)	4.73 (1.55)	5.35 (1.31)	<.001	2 > 1, 3 > 1, 4 > 1, 4 > 2
SEI	2.83 (1.45)	2.82 (1.39)	3.25 (1.53)	3.57 (1.50)	<.001	4 > 1, 4 > 2
SCI	6.14 (1.00)	5.95 (1.44)	6.14 (0.90)	6.17 (0.98)	.467	No significant differences
STA	2.43 (1.38)	2.16 (1.23)	2.15 (1.33)	1.97 (0.97)	.068	No significant differences
NCI	2.02 (1.24)	1.97 (1.20)	1.97 (1.21)	1.84 (0.96)	.721	No significant differences

Hypotheses Results

The hypotheses were also tested with SmartPLS using bootstrapping to test path coefficient significance (5,000 subsamples). The bootstrapping results for each path coefficient are shown in Table 6 and summarized graphically in Figure 2.

Table 6: PLS Results

	Path Coefficient (b)	t- statistic	p-value
CCA -> Command and Control	0.617	35.232	0.000
Command and Control -> SCI	0.101	1.759	0.079
Command and Control -> SNCI	-0.077	1.388	0.165
Command and Control -> STA	-0.043	0.806	0.420
Command and Control x SEI -> SCI	0.091	1.576	0.115
Command and Control x SEI -> SNCI	-0.014	0.212	0.832
Command and Control x SEI -> STA	0.027	0.423	0.673
Command and Control x SEN -> SCI	0.025	0.389	0.697
Command and Control x SEN -> SNCI	-0.013	0.224	0.823
Command and Control x SEN -> STA	-0.001	0.021	0.984
Command and Control x SOW -> SCI	0.008	0.121	0.904
Command and Control x SOW -> SNCI	-0.053	0.799	0.424
Command and Control x SOW -> STA	-0.038	0.635	0.526
RTB -> Command and Control	0.504	34.402	0.000
Scen1 -> SCI	-0.035	0.273	0.785
Scen1 -> SEI	-0.501	3.686	0.000
Scen1 -> SEN	-0.897	6.742	0.000
Scen1 -> SNCI	0.249	1.835	0.067
Scen1 -> SOW	-0.520	3.801	0.000
Scen1 -> STA	0.452	3.365	0.001
Scen2 -> SCI	-0.383	2.641	0.008
Scen2 -> SEI	-0.501	3.700	0.000
Scen2 -> SEN	-0.429	3.349	0.001
Scen2 -> SNCI	0.326	2.749	0.006
Scen2 -> SOW	-0.482	3.651	0.000
Scen2 -> STA	0.368	3.149	0.002
Scen3 -> SCI	-0.106	0.887	0.375
Scen3 -> SEI	-0.218	1.497	0.134
Scen3 -> SEN	-0.308	2.130	0.033
Scen3 -> SNCI	0.257	1.967	0.049
Scen3 -> SOW	-0.566	4.045	0.000
Scen3 -> STA	0.292	2.412	0.016
SEI -> SCI	-0.312	5.594	0.000
SEI -> SNCI	0.308	5.318	0.000
SEI -> STA	0.295	5.146	0.000
Self-Regulatory -> SCI	0.341	6.011	0.000
Self-Regulatory -> SNCI	-0.273	5.658	0.000
Self-Regulatory -> STA	-0.331	6.097	0.000
Self-Regulatory x SEI -> SCI	0.023	0.408	0.683
Self-Regulatory x SEI -> SNCI	-0.043	0.672	0.502
Self-Regulatory x SEI -> STA	-0.061	0.884	0.377
Self-Regulatory x SEN -> SCI	-0.049	0.640	0.522
Self-Regulatory x SEN -> SNCI	0.078	1.052	0.293
Self-Regulatory x SEN -> STA	0.087	1.144	0.253
Self-Regulatory x SOW -> SCI	-0.036	0.436	0.663
Self-Regulatory x SOW -> SNCI	-0.024	0.320	0.749
Self-Regulatory x SOW -> STA	-0.012	0.141	0.888
SEN -> SCI	-0.222	3.587	0.000

	Path Coefficient (b)	t- statistic	p-value
SEN -> SNCI	0.189	3.291	0.001
SEN -> STA	0.166	2.641	0.008
SOW -> SCI	-0.103	1.316	0.188
SOW -> SNCI	0.227	3.565	0.000
SOW -> STA	0.176	2.627	0.009
SRA -> Self-Regulatory	0.716	21.532	0.000
VC -> Self-Regulatory	0.455	16.969	0.000

Figure 2: PLS Results

Hypothesis 1 stated that higher perceptions that the policy leads to obstruction of work would be associated with (a) lower compliance intention, (b) higher noncompliance intention, and (c) higher avoidance. The PLS results indicated significant support for H1b ($b=.227$, $t=3.565$, $p<.001$) and H1c ($b=.176$, $t=2.627$, $p=.009$), but not for H1a ($b=-.103$, $t=1.316$, $p=.188$).

Hypothesis 2 stated that higher perceptions that the policy leads to lower engagement in networks would be associated with (a) lower compliance intention, (b) higher noncompliance intention, and (c) higher avoidance. The PLS results indicated significant support for H2a ($b=-.222$, $t=3.587$, $p<.001$), H2b ($b=.189$, $t=3.291$, $p=.001$), and H2c ($b=.166$, $t=2.641$, $p=.008$).

Hypothesis 3 stated that higher perceptions that the policy leads to difficulties with enactment of identity would be associated with (a) lower compliance intention, (b) higher noncompliance intention, and (c) higher avoidance. The PLS results indicated significant support for H3a ($b=-.312$, $t=5.594$, $p<.001$), H3b ($b=.308$, $t=5.318$, $p<.001$), and H3c ($b=.295$, $t=5.146$, $p<.001$).

Hypothesis 4 stated that higher self-regulatory perceptions would be associated with (a) higher compliance intention, (b) lower noncompliance intention, and (c) lower avoidance. The PLS results indicated significant support for H4a ($b=.341$, $t=6.011$, $p<.001$), H4b ($b=-.273$, $t=5.658$, $p<.001$), and H4c ($b=-.331$, $t=6.097$, $p<.001$).

Hypothesis 5 stated that higher command-and-control perceptions would be associated with (a) higher compliance intention, (b) lower noncompliance intention, and (c) lower avoidance. Perceptions about the command-and-control approach did not have significant support for H5a ($b=.101$, $t=1.759$, $p=.079$), H5b ($b=-.077$, $t=1.388$, $p=.165$), and H5c ($b=-.043$, $t=0.806$, $p=.420$).

In addition to testing the hypothesized direct effects of the command-and-control and self-regulatory perceptions, the PLS model also examined their moderating effects on adaptive and maladaptive behaviors. No significant moderating effect was found for command-and-control ($|b| \leq .091$, $t \leq 1.576$, $p \geq .115$), or self-regulatory perceptions ($|b| \leq .087$, $t \leq 1.144$, $p \geq .253$).

Discussion

This study demonstrates that employee responses to ISPs are shaped by how policies intersect with the realities of work. We examined how distinct forms of rule tension influence employees' adaptive behavior (compliance) and maladaptive behaviors (noncompliance and avoidance) toward information security policies (ISPs), and whether governance approaches shape these relationships. The results provide three key insights. First, rule tension is not a uniform construct – different dimensions exert distinct behavioral effects. Second, maladaptive behaviors can increase without a corresponding decrease in compliance intention. Third, governance approaches operate as broader motivational contexts rather than moderators of situational decision-making.

Identity-related tension exhibited the strongest and most consistent effects across all behavioral outcomes, suggesting that conflicts between ISPs and employees' professional identities were particularly influential in this context. This extends prior rule-following research by highlighting identity as a critical but underexamined driver of security behavior. In contrast, work obstruction increased maladaptive behaviors without significantly reducing compliance intention, indicating that employees may still intend to comply while simultaneously engaging in workarounds or avoidance. This distinction underscores the importance of examining multiple behavioral outcomes rather than relying solely on compliance intention as a proxy for security behavior.

The findings, which jointly examine adaptive and maladaptive responses, suggest that compliance, noncompliance, and avoidance are not simply opposite ends of a single continuum. Instead, different forms of rule tension may independently shape these behaviors, reinforcing the need for a more holistic perspective. For example, constraints on network engagement reduced compliance while increasing noncompliance and avoidance, indicating a substitution effect. In contrast, work-related tension primarily increased maladaptive behaviors without reducing compliance intention, suggesting a more complex balancing process.

Avoidance emerges as a distinct and important outcome. Employees may disengage from security decisions rather than explicitly comply with or violate policies, creating risks not captured by traditional compliance metrics. Addressing avoidance requires reducing ambiguity and complexity in security-related decision-making. These results support recent calls to move beyond binary models of compliance and toward frameworks that account for simultaneous and context-dependent responses.

Contrary to expectations, neither command-and-control nor self-regulatory approaches significantly moderate the relationship between rule tension and behavior. Instead, self-regulatory perceptions had strong direct effects on all behavioral outcomes, whereas command-and-control had no significant effects. This suggests that governance approaches operate less as situational moderators and more as overarching motivational climates. Employees who perceive ISPs as legitimate and aligned with their values are more likely to comply and less likely to engage in maladaptive behaviors, regardless of the specific tension they face. In contrast, deterrence-based approaches appear to have limited impact in contexts where employees must reconcile competing demands. This challenges assumptions about the effectiveness of enforcement mechanisms and highlights the importance of intrinsic motivation in shaping security behavior.

Limitations and Future Research

This study has several limitations that suggest directions for future research. First, the scenario-based design captures perceptions and intentions rather than observed behavior. Future research could incorporate experimental or field-based methods to examine how rule tension influences actual decision-making in real organizational contexts. Second, while this study conceptualizes rule tension as a multidimensional construct, additional forms of tension may exist. Future work could explore other situational factors, such as technological constraints or cross-organizational dependencies, that shape security behavior. Third, the absence of moderating effects for governance approaches suggests that their role may be more complex than previously theorized. Future research could examine governance as a broader organizational climate or cultural factor rather than as a situational moderator. Finally, this study focuses on individual-level perceptions. Future work could examine how team dynamics, organizational culture, and shared norms influence the relationship between rule tension and behavior.

Conclusions

This study extends prior research in information security by demonstrating that employees respond differently to distinct forms of rule tension, rather than to a uniform psychological strain. By integrating adaptive and maladaptive behaviors within a single framework, the findings show how compliance, noncompliance, and avoidance emerge from context-specific tensions between policies and work demands. While prior research has conceptualized rule tension as a general psychological state, the results show that obstruction of work, constraints on network engagement, and identity enactment tensions influence behavior in distinct ways. Rather than viewing noncompliance as a failure of awareness or enforcement, the findings suggest that it often reflects rational responses to competing demands. Addressing this challenge requires policies and governance approaches that acknowledge the complex, situated nature of employee work.

Improving security behavior requires addressing the sources of rule tension rather than relying solely on enforcement or awareness. Policies that obstruct work, limit collaboration, or conflict with professional identity are likely to generate maladaptive responses even when employees intend to comply. Organizations should therefore focus on aligning ISPs with work processes, collaboration needs, and role expectations. Particular attention should be given to identity-related tensions, as these appear to have the strongest behavioral effects. Additionally, the results suggest that command-and-control approaches alone are insufficient; fostering self-regulation through clear justification, communication, and value alignment may be more effective in shaping behavior.

References

- Aguinis, H., & Bradley, K. J. (2014). Best practice recommendations for designing and implementing experimental vignette methodology studies. *Organizational Research Methods*, 17(4), 351–371.
- Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences*, 11(8), 3383. <https://doi.org/10.3390/app11083383>
- Ament, C., & Haag, S. (2016). Security-related stress – a neglected construct in information systems stress literature. *Proceedings of HAISA*, 12–21.
- AnuPriya. (2025, April 17). 33,000 employee records exposed in data leak from tech service provider. *Cyber Security News*. <https://cyberpress.org/employee-records-exposed-in-data-leak/>
- Ayyagari, R., Grover, V., & Purvis, R. (2011). Technostress: Technological antecedents and implications. *MIS Quarterly*, 35(4), 831–858.
- 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. *Proceedings of HAISA*, 12–21.
- 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. (Robert), & Li, H. (2022). Beyond adaptive security coping behaviors: Theory and empirical evidence. *Information & Management*, 59(2), 103575.
- D’Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, 31(2), 285–318.
- 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.
- Down, A. (2026, March 20). Meta AI agent’s instruction causes large sensitive data leak to employees. *The Guardian*. <https://www.theguardian.com/technology/2026/mar/20/meta-ai-agents-instruction-causes-large-sensitive-data-leak-to-employees>

- Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, 28(2), 203–236.
- Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, 19(2), 139–152.
- 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., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems*, 20(4), 373–384.
- Hodges, D., Haines, R., & Agrawal, D. (2024). To follow the rules or break them: An individual rule-following perspective. *Issues in Information Systems*, 25(2).
- 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), 99–110.
- 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.
- Intelligence, M. D. S. R. T., & Microsoft Threat Intelligence. (2026, May 4). Breaking the code: Multi-stage ‘code of conduct’ phishing campaign leads to AiTM token compromise. *Microsoft Security Blog*. <https://www.microsoft.com/en-us/security/blog/2026/05/04/breaking-the-code-multi-stage-code-of-conduct-phishing-campaign-leads-to-aitm-token-compromise/>
- 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.
- Li, H., & Huang, K. (2020). The role of emotion-focused coping in information security policy violations: A stress-coping perspective. *Information & Management*, 57(6), 103345.
- Liang, H., Xue, Y., & Wu, L. (2019). Ensuring employees’ information security compliance: A fit-viability model. *Information Systems Research*, 30(2), 481–501.
- Liu, Y., Yu, C., Sheng, J., & Zhang, T. (2018). Self-collision avoidance trajectory planning and robust control of a dual-arm space robot. *International Journal of Control, Automation, and Systems*, 16(6), 2896–2905.
- Myrsky, L., Siponen, M., Pahlila, 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*, 34–44.

- Ragu-Nathan, T., Tarafdar, M., Ragu-Nathan, B. S., & Tu, Q. (2008). The consequences of technostress for end users in organizations: Conceptual development and empirical validation. *Information Systems Research*, 19(4), 417–433.
- Ringle, C. M., Wende, S., & Becker, J.-M. (2022). *SmartPLS 4* [Computer software]. <https://www.smartpls.com>
- 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), 1438–1451.
- Sarstedt, M., Hair, J. F., Jr., & Ringle, C. M. (2023). PLS-SEM: Indeed a silver bullet – retrospective observations and recent advances. *Journal of Marketing Theory and Practice*, 31(3), 261–275.
- Siponen, M., & Iivari, J. (2006). Six design theories for IS security policies and guidelines. *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), 296–302.
- Splunk. (2023). *The state of security*. https://www.splunk.com/en_us/pdfs/gated/ebooks/state-of-security-2023.pdf
- Tyler, T. R. (2006). Psychological perspectives on legitimacy and legitimation. *Annual Review of Psychology*, 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.
- Verizon. (2023). *Data Breach Investigations Report*. <https://www.verizon.com/business/resources/reports/dbir/>
- Yazdanmehr, A., Li, Y., & Wang, J. (2023). Employee responses to information security-related stress: Coping and violation intention. *Information Systems Journal*, 33(3), 598–639.
- 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*.