Winter 12-10-2023

To Follow the Rules or Break Them: A Rule Following Perspective

Darin Hodges
Appalachian State University, agrawald@appstate.edu

Deepti Agrawal
Appalachian State University

Russell Haines
Appalachian State University

To Follow the Rules or Break Them: A Rule Following Perspective

Darin Hodges
Walker College of Business, Appalachian State University, Boone, NC, USA

Deepti Agrawal[1]
Walker College of Business, Appalachian State University, Boone, NC, USA

Russell Haines
Walker College of Business, Appalachian State University, Boone, NC, USA

ABSTRACT

Because most security breaches are caused by human error, employees are perceived as the first line of defense against threats. Accordingly, organizations invest in information security policy (ISP) creation, implementation, and training initiatives. However, despite a vast stream of research, employee compliance with the information security policy remains an issue. We argue that it is not enough to study the motivations behind ISP compliance, since the motivation for adaptive behavior (ISP compliance) may be different from 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 approach 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 breaches began through human error, social engineering, or misuse (Verizon, 2023), implying that employees remain the biggest threat to

[1] Corresponding author. agrawald@appstate.edu +1 828 262 7444

information security. The routine interaction between the employees and the organization's systems and data can either create vulnerabilities or help safeguard the organization's security efforts. Recognizing this, most organizations have invested in information security policies (ISP) implementation and training to make the employees their first line of defense against cyberattacks. However, the policies are only effective to the extent to which they are followed. Even if just one employee disregards a rule, takes a shortcut, or makes an error in judgment, it can lead to a security breach.

A vast stream of research has looked at factors motivating employee's compliance with Information security policies. However, most of these studies treat non-compliance as the opposite of compliance and have thus mostly focused only on ISP compliance (e.g., Bulgurcu et al. 2010; Yazdanmehr et al. 2020). Recently a few studies have suggested that an employee's motivations for adaptive behaviors such as compliance may not be the same as those for maladaptive behaviors such as non-compliance (Chen et al. 2022), highlighting the pressing need for a more holistic approach that can account for both adaptive and maladaptive behaviors towards ISP. Further, recent research (Karjalainen et al. 2019) highlighted the need for investigating the tension caused by differing goals and interests between individual employees and the organization which may lead individuals to balance environmental conditions or situational demands with compliant, partially compliant, or non-compliant decisions.

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 and 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 and Robertson 2015). One reason behind the employees not following the organizational rules is that the requirements of the rules disrupt their work (Hannah and 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 and 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. Considering this recent Information Systems literature that underscores the need for more exploration of rule tensions in the workplace and their impact on adaptive or 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 why and how behind the employee' decision to follow or go against the information security policies of their organizations when they face rule tension. More specifically,

RQ: How do the command-and-control and self-regulatory approaches influence an employee's behavior towards information security policy when faced with rule tension?

THEORETICAL BACKGROUND AND RESEARCH MODEL

Hannah and Robertson (2015) identified three types of rule tension – work obstruction, knowledge network tension, and 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 and Robertson 2015). Rule tension associated with engagement in knowledge networks is related to policies that prevent the flow of information sharing. It could lead to preventing the sharing of information with colleagues (internal network) and to falling behind on technology, being left out of collaborations, or missing out on valuable feedback (external network). An employee may face identity tension when the rules outlined in the ISP do not align with the values or identity of the employees. Based on prior literature (D'Arcy et al. 2014; D'Arcy and Lowry 2019; D'Arcy and Teh 2019; Myyry et al. 2009), some of the ways in which employees may experience rule tension in the context of information security may include slowing down of 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).

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 and 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 and Robertson 2015). Hence, we hypothesize,

H1: The employees who perceive rule tension because of (a) obstruction of work, (b) engagement in networks, and (c) enactment of identity are less likely to exhibit adaptive behaviors towards ISP compliance.

H2: The employees who perceive rule tension because of (a) obstruction of work, (b) engagement in networks, and (c) enactment of identity are more likely to exhibit maladaptive behaviors towards ISP compliance.

The command-and-control approach assumes an economic view of human behavior and actions, indicating that people engage in a cost-benefit analysis and attempt 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.

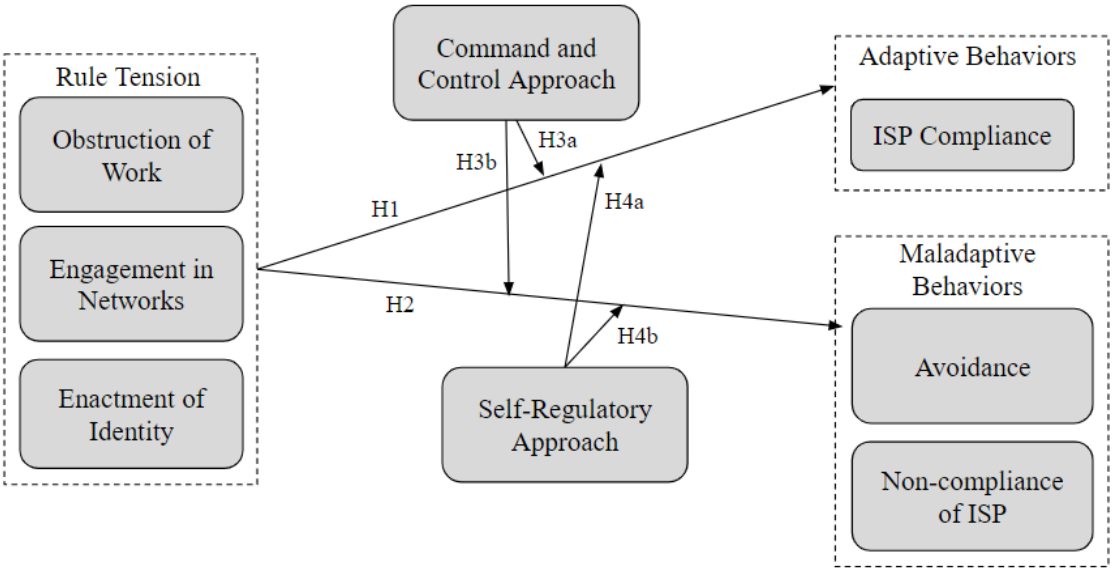

Figure 1. Research Model

RESEARCH METHODS

The research model for this study is shown in Figure 1. A survey-based experiment will be used to test the hypotheses. Knowledge workers will be recruited via a panel survey company such as Qualtrics. Screening questions will determine whether potential respondents are employed in companies where there is an information security policy. Pre-existing, validated questionnaire instruments will be adapted for the survey.

Two outcomes are expected in the research model. Adaptive Behaviors consist of ISP compliance intentions (Chen et al. 2021) (e.g., " I intend to comply with the requirements of the

Information Security Policy"). Maladaptive behaviors (Chen et al. 2021) consist of (1) avoidance (e.g., “If I were told about what can happen to my organization and what can happen to me if I were to purposely not comply with my organization’s information security policy, my first instinct is to ignore or disregard the potential threats to me and my organization”), and (2) ISP noncompliance intentions (e.g., " I intend to NOT carry out my responsibilities prescribed in the requirements of the Information Security Policy").

The independent variable rule tension based on Hannah and Robertson (2015) is measured 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 will be collected. Command-and-control approach (Yazdanmehr et al. 2020) is comprised of (1) Detection of Behavior (e.g., "How closely is your work monitored by your organization?"), and (2) Reaction to Behavior (e.g., "If you were caught breaking the organization's ISP, how much would your organization care?"). Self-Regulatory Approach (Yazdanmehr et al. 2020) is comprised of (1) Legitimacy (e.g., "Work organizations are most effective when people follow their organization's Information Security Policy") and (2) Value Congruence (e.g., "I find that my values and the values where I work are very similar").

DISCUSSSION AND CONCLUSION

The results of the study are expected to have the following contributions. First, this study proposes a model that accounts for both adaptive (compliance) and maladaptive (avoidance and non-compliance) behaviors together in the context of behavioral information security research,

thus proposing dual coping outcomes. By taking a more holistic approach which has received less attention in information security research, we address a call made by Chen et al. (2022). Second, our research model is based on the rule-following perspective in the context of information security, which has not been used previously. Third, it identifies three types of tensions that employees can face with regard to following information security rules: obstruction to their work, their engagement in external and internal networks, and their identity enactment. As noted above, the study proposes that the relationship between the rule tension and the rule-following (adaptive or maladaptive) behaviors can be moderated by two approaches – command-and-control and self-regulatory. Utilization of command-and-control and self-regulatory approaches are rarely investigated as relationship enhancers in the greater IS literature. 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 the study are expected to shed further light on which approach works better under which situation or whether these approaches work together in a complementary manner. Thus, our findings are expected to add to the literature a more nuanced connection between these two approaches than previously understood.

Finally, the study also offers relevant practical insights. Many users consider security-related tasks as a barrier to getting their work done, engaging with important others within the organization and outside, or enacting their identities. Awareness of these rule tensions will help the managers and IS function design information security policies and procedures in a better way to reduce the rule tension for employees. It will also help the practitioners understand the implications of different strategies used by the employees to cope with the tensions and thus possibly be able to address these through proper communication and training.

REFERENCES

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523-548.

Chen, Y., Galletta, D. F., Lowry, P. B., Luo, X., Moody, G. D., and 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), pp. 1043-1065.

Chen, Y., Luo, X. R., and Li, H. 2022. "Beyond Adaptive Security Coping Behaviors: Theory and Empirical Evidence," *Information & Management* (59:2), p. 103575.

D'Arcy, J., Herath, T., and Shoss, M. K. 2014. "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," *Journal of Management Information Systems* (31:2), pp. 285-318.

D'Arcy, J., and Lowry, P. B. 2019. "Cognitive-Affective Drivers of Employees' Daily Compliance with Information Security Policies: A Multilevel, Longitudinal Study," *Information Systems Journal* (29:1), pp. 43-69.

D'Arcy, J., and 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), p. 103151.

Hannah, D. R., and Robertson, K. 2015. "Why and How Do Employees Break and Bend Confidential Information Protection Rules?," *Journal of Management Studies* (52:3), pp. 381-413.

Karjalainen, M., Sarker, S., and Siponen, M. 2019. "Toward a Theory of Information Systems Security Behaviors of Organizational Employees: A Dialectical Process Perspective," *Information Systems Research* (30:2), pp. 687-704.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and 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), pp. 126-139.

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

Verizon. 2023. "Data Breach Investigations Report," https://www.verizon.com/business/resources/reports/dbir/#resources.

Yazdanmehr, A., Wang, J., and Yang, Z. 2020. "Peers Matter: The Moderating Role of Social Influence on Information Security Policy Compliance," *Information Systems Journal* (30:5), pp. 791-844.