

# **Exploring the Cognitive Comfort Zone of Compliance with Information Security Policies: A View from Cognitive Continuum**

**Early stage paper**

**Weijie Zhao**  
University of Alabama  
wzhao19@ua.edu

**Allen Johnston**  
University of Alabama  
acjohnston5@ua.edu

**Mikko Siponen**  
University of Alabama  
tmsiponen@ua.edu

## **ABSTRACT**

Ensuring the long-term effectiveness of employee compliance with information security policies is still a challenge for organizations. Changes in making compliance decisions are associated with cognitive change in accordance with specific security tasks and environments. We plan to conduct an 8-week longitudinal study to explore the most beneficial cognitive mode for employees to comply with password protection policies in the workplace over time. We proposed that quasirationality would be that mode referred to as cognitive “comfort zone” which would ensure consistent security behavior and mitigate cognitive disorders that are caused by strict security requirements. This study will contribute to investigating long-term compliance from a decision-making view and provide a cognitive explanation of inconsistent findings from only measuring short-term compliance. Implementation of effective security interventions such as security training, monitoring, and feedback needs not only behavioral change but also cognitive change.

## **Keywords**

Compliance, information security policy, quasirationality, cognitive continuum, longitudinal design.

## INTRODUCTION

Despite significant investments in advanced technical safeguards and strong behavioral controls, insider threats remain a huge challenge in organizational security management (Burns et al. 2023). The persistence of insider threats highlights the need for organizations to implement effective security controls such as information security policies (ISPs) to address human errors from internal employees. ISPs vary in response to diverse security threats, organizational responsibilities, and goals (Paananen et al. 2020). Organizations employ multiple approaches such as security education, training, awareness programs (Burns et al. 2018; Hu et al. 2021a), persuasion messages (Boss et al. 2015; Johnston et al. 2015, 2023), and deterrence techniques (Aurigemma and Mattson 2017; Burns et al. 2023; D’Arcy et al. 2009) to motivate employee compliance with ISPs. However, when employees encounter environmental factors that challenge their existing security behavior, they may change current compliance decisions (Li et al. 2021). For example, in a high workload environment, to balance time and energy to satisfy job performance and security needs, employees may change account passwords but fail to follow security requirements by writing the new passwords down on a note to minimize the memorable load (Sarkar et al. 2020). Their security decisions may oscillate between full compliance and noncompliance to find a comfort zone of cognition over time.

Compliance with ISPs is not a simple time-point binary decision, but rather a process of behavioral change that aligns with personal traits and perceived environmental characteristics (Cram and D’Arcy 2023). Employees’ understanding of ISPs and perceived compliance environment influence their security behavior over time (O’Connor et al. 2023). Studying employee compliance with ISPs in a cross-sectional design helps to explain motivational variances and explore causal relationships between antecedents and consequences but lacks

identification and investigation of behavioral change in a dynamic security environment (Cram et al. 2024; Karjalainen et al. 2019). To address such weakness with enhancing intrapersonal explanations for behavioral change, researchers conducted longitudinal studies rather than cross-sectional surveys to examine compliance process (see Appendix A). These studies measure employees' security behavior over multiple periods to test the behavioral consistency of compliance. From them, we found that environmental, personal, and policy-related factors initially influence employees' cognition of security tasks, which then leads to specific compliance decisions in response to security threats and requests. Thus, to investigate behavioral changes of compliance, it is necessary to explore cognitive change of security tasks.

Individuals respond to security threats relaying on two cognitive modes which are intuitive mode and analytical mode (Slovic et al. 2004). Intuitive mode is regarded to be rapid, unconscious, inconsistent, and moderately accurate data processing, requiring little cognitive effort; while analytical mode is regarded as slow, conscious, consistent, and accurate data processing, requiring much cognitive effort (Dhimi and Thomson 2012). When employees lack appropriate knowledge of ISPs and security practices, they may suffer uncertainty and anxiety (Kim and Kim 2017), leading to fast security decisions based on personal experience and feelings without much thought. The underlying cognitive process would be an intuitive mode. As a result, relevant security behaviors are susceptible to personal characteristics, environmental changes, and emotions (Slovic et al. 2004), easily leading to inconsistent security behaviors over time. To help employees understand security requirements and practices of ISPs, organizations implement security training to strength their security awareness (Hu et al. 2021b). At the same time, to motivate strict compliance, sanctions of noncompliance and monitoring of actual security behaviors are employed. With such intensive security controls, employees change to

adopt an analytical mode in responding to the security requirements of ISPs. However, the conflicts between security practices and job tasks may cause cognitive overload, decision fatigue, and security stress (Nobles 2022), reducing employees' actual compliance outcomes.

In security practices, employees' cognition is usually a combination of intuition and analysis, which jointly influence the end security behavior (Dennis and Minas 2018). Cognitive uncertainty generated by changes in security environments and ambiguous policy understanding induces intuitive judgements, which lead to low consistency and confidence in security decisions (Dhami and Thomson 2012; Newell and Shanks 2014). Complex security procedures and strict security controls prompt analytical thinking, resulting in security overload and mental disorders (Alecse 2023; Dhami and Thomson 2012; Nobles 2022). Thus, there is a critical need for employees to have a balanced state of security cognition that is neither purely intuitive nor purely analytical (Tsohou et al. 2015). We regard it as employees' cognitive comfort zone for compliance with ISPs. From cognitive continuum theory, it is defined as "quasirationality", combining the common characteristics of intuitive and analytical modes (Hammond 1980, 1981).

However, current security studies have not discussed how to identify and measure that cognitive mode (i.e., quasirationality) and how to mitigate above negative consequences caused by purely intuitive or analytical in compliance with ISPs. Thus, it is necessary to identify the cognitive comfort zone for employees to comply with ISPs over time and what factors influence their cognitive processes to move into the comfort zone, which help use to develop effective behavioral strategies and cognitive interventions to promote long-term and effective security practices for employees (Ifinedo 2014; Safa et al. 2016; Yazdanmehr and Wang 2016). We ask two research question: *Whether quasirationality is the most appropriate security cognitive mode*

*for employees to comply with ISPs over time? How to motivate employees to move into that cognitive mode?*

To address the above two research questions, we will derive from cognitive continuum theory (CCT; Hammond, 1980) and employ a longitudinal study with an experienced sampling method (ESM; Cram et al., 2024) to explore the cognitive comfort zone for long-term compliance with ISPs and to examine the effective cognitive interventions.

This study will contribute to theory and practice in the following aspects. First, this study extends our understanding of compliance with ISPs to a long-term view of behavioral consistency associated with cognitive modes rather than a time-point requirement matching. Second, this study emphasizes the importance of a balanced cognitive state as the comfort zone for security practices to maintain consistent compliance over time and mitigate potential security mental disorders. Third, this study supports the view that contextual factors are taken into account when considering the attributes of different ISPs in a dynamic security environment. The inconsistent research findings may result from measuring actual compliance behavior at different time points and across security contexts (Aurigemma and Mattson 2019). Fourth, this study argues for a continuum view of security cognition rather than a dual process in making security decisions. Fifth, organizations need to assess the cognitive modes of employees when adopting security controls to implement effective security training and monitoring approaches. In particular, security interventions relevant to different ISPs should vary according to the characteristics of security environment and practices.

## **THEORETICAL FOUNDATION AND HYPOTHESES**

### **Long-term compliance with ISPs**

Most IS studies employ a cross-sectional view to understand organizational and individual factors that motivate employee compliance with ISPs, lacking a persistent intervention in the compliance process (Cram et al. 2017). Investigating how to motivate employee compliance behavior with a focus on the persistence of compliance becomes an attractive topic when researchers discuss the actual security effects derived from current theories that fail to explain employee security behavior over time (Cram et al. 2024).

Belanger et al. (2017) examined the impact of early compliance in the context of password change and found its significant impact on continuous compliance behavior influenced by employees' attitudes toward ISPs. Derived from protection motivation theory, Warkentin et al. (2016) found that perceived threat severity and susceptibility, and self-efficacy had a significant impact on the ongoing use of anti-malware software. In comparing formal and informal sanctions derived from deterrence theory, Hengstler et al. (2023) found that employees are sensitive to being detected for deviant behavior in long-term security practices. By considering both cognitive and affective factors, D'Arcy & Lowry (2019) found their integrative impact on motivating employees to comply with ISPs over time and that the inclusion of factors associated with moral considerations strengthens this long-term impact. Continuing to dig into the negative impact of psychological and affective factors, D'Arcy & Teh (2019) demonstrated that employees' suffering from persistent security stress leads to their feelings of security frustration and fatigue, further neutralizing coping responses that fail to comply with ISPs over time.

For employees to comply with ISPs over time, continuous security behavior (Warkentin et al. 2016a), ongoing monitoring (Hengstler et al. 2023b), and proactive commitment (D’Arcy and Lowry 2019) are important factors in facilitating consistent compliance over time. Thus, we define long-term compliance with ISPs as employees continuously monitoring their security behaviors to be aligned with ISPs, with a focus on proactive persistent commitment rather than passive initial actions. Long-term compliance outlines the cumulative effects of security performance, including the formation of security awareness (Aggeliki Tsohou and Kiountouzis 2015), habits (Vance et al. 2012, 2018; Venkatesh et al. 2023), and beliefs (D’Arcy and Lowry 2019; Vance et al. 2020). Continuous compliance focuses on comparing behavioral identification before and after an observation period, whereas long-term compliance reflects employees’ relatively fixed state of security behavior in contributing to security outcomes, even if it is affected by unexpected events or emotions that away from full compliance.

Long-term compliance is involved with the continuous evaluation of security environments and current security behavior, which is an ongoing decision-making process associated with cognitive change. In healthcare, this view was discussed from the perspective of the cognitive-motivational process which refers to the extent to which compliance behaviors are active, intentional, and responsible processes (Kyngas et al. 1996). Karjalainen et al. (2019) used a dialectical process model to describe how employees balance the cognitive tension of environmental and individual factors to determine their security behaviors. According to this particular study, security behavior is not a dichotomy of compliance or noncompliance but changes as variances with specific situations and ISPs. From the intuitive reaction to the routine repetition, employees change the stage of security behavior influenced by both individual and organizational factors (Karjalainen et al. 2020). The interplay between cognitions and situational

factors, including time constraints, task complexity, and perceived security primacy, shapes employees' long-term compliance decisions (Aurigemma and Mattson 2018; Butavicius et al. 2022; Vance et al. 2022).

### **Cognitive continuum theory (CCT)**

CCT is considered an adaptive theory of a decision-making process that focuses on the dynamic relationship of the organism-environment interaction (Dunwoody et al. 2000). Unlike dual-process theory, which treats intuition and analysis as two independent cognitive processes from a dichotomous perspective (Evans and Stanovich 2013), CCT places an individual's cognition on a continuum. CCT identifies three cognitive modes: intuition, analysis, and quasirationality, with intuition and analysis at opposite ends, and the middle zone referred to as quasirationality (Hammond 1981, 1996). Typically, people in the intuitive mode tend to simply average out available information, whereas people in the analytical mode may combine information in more complicated ways using organizational principles (Hammond et al. 1987). Quasirationality consists of different combinations of intuition and analysis in that cognitive continuum. Beyond simply combining intuition and analysis, quasirationality integrates an individual's cognitive states in a discontinuity-free manner (Conlon et al. 2023), considered a widespread and beneficial cognitive mode in management when individuals make a decision (Dhami and Thomson 2012).

In the cognitive continuum identified from CCT, cognitive mode is not static but oscillates between intuition and analysis in response to changes in relevant tasks and environments (Dunwoody et al. 2000). Functional relationships, pattern recognition, and the degree to which task properties match cognitive properties determine cognitive performance that influenced the end decision-making (Conlon et al. 2023; Dhami and Mumpower 2018;



Hammond 1996; Hammond et al. 1987; Standing 2008). People with a quasirational mode deal with information in a way that takes inherent experience and organizational core guidelines, and they make the appropriate decisions after evaluating the current environment (Dhami and Thomson 2012).

## **Hypotheses development**

Under time pressure, employees make quick decisions based on personal experience or feelings without thinking, prioritizing productivity over security, leading to neglect or partial compliance (Allen 2011; Alter 2015). Cognitive conflict between work and security may be exacerbated when lack of adequate security knowledge and weak understanding of ISPs induces reliance on intuitive judgments (Lipshitz and Strauss 1997). Over time, intuitive responses to security requirements will lead to low compliance consistency, which contribute to negative impacts on security practices (Nobles 2022). Thus, we hypothesize that:

H1: Time pressure increases the preference for an intuitive mode to respond to security requirements.

H2: Employees who use an intuitive mode to respond to security requirements have decreased compliance consistency over time.

H3: Consistency of compliance with ISPs is positively associated with compliance effectiveness.

In contrast, employees who rely on an analytic mode are meticulous and structured in complying with ISPs (Alter 2015). Analytic decision-making leads to a thorough assessment of security tasks and environments. Often, more complex tasks require more cognitive engagement for slow analysis (Standing 2008). Because of the strict compliance with security procedures, compliance patterns are well established and cannot be easily changed. However, over time, such

analytic mode toward security behavior may exacerbate security cognitive overload as environments and policies change, leading to a decline in compliance effectiveness (Cram et al., 2021; D'Arcy et al., 2014). Thus, we hypothesize that:

H4: Task complexity increases the preference for an analytic mode to respond to security requirements.

H5: Employees who use an analytic mode to respond to security requirements have increased security cognitive overload over time.

H6: Security cognitive overload is negatively associated with compliance effectiveness.

Beyond the above two modes, employees may use a quasirational mode to comply with the core requirements of ISPs and consider contextual factors to make compliance decisions (Siponen and Iivari 2006). Flexibility in the decision-making process allows employees to combine the properties of intuition and analysis to make appropriate security decisions (Hammond 2010). Quasirationality relies on personal security experience and the requirements of ISPs, combining the strengths of intuition and analysis to mitigate cognitive disorders as well as to ensure the implementation of ISPs. In a cognitive continuum, quasirationality is regarded as the most beneficial cognitive mode to ensure task performance and accuracy of judgment (Dunwoody et al. 2000). Thus, we hypothesize that:

H7: Employees who use a quasirational mode to respond to security requirements have better compliance effectiveness than those who use an intuitive or analytic mode over time.

## **METHODOLOGY**

### **Longitudinal design**

An ESM has been used to capture daily-level behavioral changes in employee compliance with ISPs to investigate the security behavioral tendencies by enhancing intrapersonal explanations (Cram et al. 2024; D’Arcy and Lowry 2019; D’Arcy and Teh 2019). However, the timeframe of the investigations varied from study to study. Researchers asked participants to complete a diary survey to measure compliance in a given security context in two (D’Arcy and Lowry 2019), three (D’Arcy and Teh 2019), four (Cram et al. 2024), or even eight weeks (Boss et al. 2015). To mitigate the response fatigue, they distributed the survey in appropriate time intervals, such as three times per week, resulting in 9 to 12 surveys per person (Cram et al. 2024; D’Arcy and Teh 2019), which still satisfied the time validity for effective measurement of actual behavior (Fisher and To 2012). To measure actual behavior over time, researchers suggested an at least two-month duration for capturing objective security behavior (Belanger et al. 2017; Boss et al. 2015; Warkentin et al. 2016b). Thus, our initial investigation will last for 8 weeks.

To adopt a similar approach to reduce response fatigue, we considered appropriate survey intervals. Security performance has a similar weekly effect to job performance in that employees feel tired and fatigued on the last day of the workday (Cram et al. 2024; Diestre et al. 2020). To ensure the validity of the results of exploring the cognitive comfort zone, it is preferable to capture the upper limit of the cognitive load during the workday to demonstrate that the most appropriate cognitive mode attenuates the threshold. In our case, Fridays are the appropriate day to take surveys at intervals of one week. Thus, we plan to conduct an eight-week longitudinal study where participants will only be asked to answer questionnaires on Fridays, to investigate cognitive and behavioral changes in their compliance with ISPs.

We expect to examine specific security behaviors required by ISPs in which employees' cognitive modes may change according to the way security practices and environmental controls are implemented. Username-password logins are widely used for credential identification with features of ease of use and management. However, as password cracking techniques evolve, the tension between convenience and security is highlighted when employees are forced to choose complex and unique passwords for a single security threat (Rieger et al. 2024). Password manager could be a good way to mitigate such tension because it helps release individuals' memory load and secure the password storage. Thus, we chose password management as the security context and the use of password managers as the manipulation to investigate the security performance of three cognitive groups.

## Research setting

We will differentiate cognitive approaches based on password choice (whether to use easy-to-remember passwords), password reuse (whether to use the same password for multiple accounts), and password storage (whether and how to use password managers). We provide an approved password manager “Keeper” for participants to generate and store passwords. Participants' cognitive mode underlying their password management decisions will be induced by requirements for different levels of Keeper usage (see Table 1).

	<b>Intuitive Approach (Group 1)</b>	<b>Analytical Approach (Group 2)</b>	<b>Quasirational Approach (Group 3)</b>
<b>General password use</b>	Participants log in to workstations using their work accounts and passwords. The previous 5 passwords cannot be used. 10 failed login attempts will cause account lock for at least 15 minutes.		
<b>password choice</b>	All passwords are self-selected following a given ISP.	All passwords are auto-generated by Keeper.	Passwords for work accounts are auto-generated by Keeper and other work-related accounts can be self-selected following a given ISP.
<b>password reuse</b>	There are no requirements on preventing from the use	Auto-generated passwords are different for any account.	Auto-generated passwords are different for work accounts and self-selected passwords are not

	of the same password for multiple accounts.		allowed to be used for multiple accounts.
<b>password storage</b>	No restrictions on the use of password managers	Mandatory use of Keeper to store all passwords	Mandatory use of Keeper to store passwords for work accounts and optional use of it to store other passwords

**Table 1. Cognitive groups in password management.****Measurement**

In response to the call to measure actual behavior (Aurigemma and Mattson 2019), we would like to record participants' actual security practices when measuring compliance with ISPs to reduce errors in self-reported information. Precedents for capturing actual security behavior exist, including tracking individuals' use of anti-malware software through custom-built security applications Warkentin et al. (2016), and automated logs of individuals' backup activities through existing systems Boss et al. (2015). To measure actual security behavior for password management, we will track participants' password use and storage activities, including the number of accounts that use the same password (password reuse), the number of passwords saved in Keeper, the number of passwords saved in browser extensions including Keeper and others, the number of passwords reset (forget frequency), and the number of accounts used for work. We will also track employees' login/out activities including time, frequency, failed attempts, and locations as control variables.

Cognitive modes will be measured by using the Cognitive Style Index (CSI; Allinson and Hayes 1996). The survey questions can be found in Appendix B. The closer an individual's total CSI score is to the maximum score of 76, the more analytical they are; the closer the total CSI score is to the minimum score of 0, the more intuitive they are; a quasirational mode is in the middle range (see Table 2). The personal and environmental factors will be measured using the existing instruments (Liu et al. 2020; Tyler and Blader 2005).

	<i>Cognitive mode</i>	<i>Score range</i>
<i>Intuition</i>	Intuitive	0 -28
	Quasi-Intuitive	29 – 38
<i>Quasirationality</i>	Adaptive	39 – 45
	Quasi-Analytic	46 – 52
<i>Analysis</i>	Analytic	53 - 76

**Table 2. CSI score ranges for cognitive modes** (Allinson and Hayes 2011).

## Research procedure

Prior to conducting the longitudinal study, we will run a pretest with 15 graduate students at a public university in the United States to assess the manipulative effects of the tasks on three cognitive modes and the validity of the measurements. The procedures for the pretest study will be identical to the formal cognitive tasks. At the end of the pretest, students will be asked to complete a follow-up survey to provide feedback on the longitudinal design.

We plan to follow four steps to run the study. In step 1 (baseline data), we will collect initial data on participants' current password management habits, decision-making styles for compliance with ISPs, and demographic information, before assigning them into three cognitive groups. In step 2 (group), we will assign 60 participants to 3 cognitive groups at the beginning of the first week and give them a week to immerse in password management activities including login/out with credentials and storage. In step 3 (implementation), we will roll out the respective policies and associated requirement of using Keeper to each group on the Monday of the second week, ensuring clear communication of the requirements for all participants. In step 4 (ongoing tracking), for 2 months from the day of the assigned group, we will track logs of password use and storage daily, responses to surveys weekly, and continued compliance monthly. Participants

who fail to respond to the weekly survey on three attempts will be removed from the data analysis and will be considered a failure to continue compliance for the associated group.

### **Proposed analysis approach**

By collecting longitudinal data, we can quantitatively assess how different cognitive modes affect long-term compliance with ISPs at both an intrapersonal and interpersonal level (D'Arcy and Lowry 2019). Intrapersonal level analysis focuses on examining the impact of cognitive modes on behavioral change within an employee, emphasizing individual unique context for compliance with ISPs over time. Interpersonal level analysis compares the impact of cognitive modes across different populations on long-term compliance with ISPs, focusing the explanation of variances on personal and environmental factors. We will use latent growth models to analyze survey data with temporal variation (Serva et al. 2011) and parametric regression to analyze logs of password management (Wang et al. 2015).

## **DISCUSSION AND EXPECTED IMPLICATIONS**

Long-term concerns about compliance with ISPs have emerged. Cram et al. (2024) used an idiosyncratic approach to examine the with-person factors that influence employees' long-term compliance with ISPs. Our study coincides with this theoretical perspective and aims to understand individuals' unique contexts and relevant environmental factors in the long-term compliance process. By conducting both interpersonal and intrapersonal analysis, we provide a holistic view of studying employees' security behavior over time. In exploring long-term compliance, employees' cognition of security tasks and surroundings influences their actual compliance behavior. Many factors lead to inconsistent compliance, but the first of these factors to be influenced is their cognitive mode. Exploring the cognitive mode of employee compliance allows for new perspectives in explaining the inconsistent results of security interventions over

time. By integrating the influence of human and environmental factors on employees' cognitions of compliance, we open a new path for investigating behaviors that oscillate between noncompliance and compliance. Understanding the cognitive processes behind such behavioral changes can provide concrete guidance for the implementation of tailored interventions and policies to more effectively respond to security threats that arise in changing environments.

Also, we compare differences in compliance across groups with different cognitive modes. From a cognitive perspective, it will help address psychological weaknesses such as security fatigue and burnout that occur in compliance over time (Nobles 2022). In particular, we find that the emergence of security fatigue and reactance is related to goal ambivalence and that the nature of this is a mismatch between cognitive modes and security task characteristics. Finding the most appropriate cognitive mode as the environment changes is an effective way to address mental disorders caused by security behaviors. When an employee's cognitive mode for engaging in security behaviors is highly matched with the characteristics of the security task required by the organization, the security task that appears to conflict with the work goal does not significantly mitigate the employee's security intentions. Our study contributes to marking such cognitive “comfort zone” for employees to maintain a persistent compliance behavior.

Employees' cognitive change is highly sensitive to time pressure. When implementing ISPs, excessive time pressure can make employees prefer to rely on intuitive judgment, which can result in quick completion of security requirements but make it difficult to ensure completeness and accuracy. At the same time, employees can easily feel overloaded and burdensome if too much time pressure is applied to complex security tasks. On the other hand, excessive time relaxation would allow employees to neglect security tasks and fail to achieve the desired security goals. Thus, appropriate time pressure is necessary to maintain comfortable



employee compliance, and organizations need to implement monitoring and feedback on employee perceptions of time.

Previous security experience and familiarity with ISPs are important factors in motivating employees to follow security requirements. Employees who lack a comprehensive understanding of ISPs and appropriate approaches to comply tend to adopt initiative mode based on personal experiences and feelings. Its immediate effects on compliance do not ensure long-term effectiveness. Usually, employees' security experiences may not align with organizational security requirements (Karjalainen et al. 2020). Although such employees have no intentions to harm organizational information assets, they cannot be recognized for their compliance behavior. A security education, training, and awareness program plays an important role in improving such a situation (Hu et al. 2021a). Security management can spread the importance of information security and popularize the existing ISPs from time to time to enhance employees' understanding and perceived importance of ISPs. Also, resources permitting, a stand-alone security training department can be established to provide regular information security training and daily information security services to employees.

Employee cognition of compliance with ISPs changes depending on individual and environmental factors. Beyond enhancing policy understanding and security training, organizations need to consider security interventions that are rooted in employees' daily routines. For example, reminders from coworkers and daily monitoring by managers can subconsciously influence employee compliance cognition. Also, by guiding employees to take on security responsibilities and roles in protecting organizational information assets, organizations can advocate for employees to self-initiate security cognition and reinforce the importance of compliance with ISPs in their daily work (Frank and Kohn 2023).

The extent to which employees' compliance cognition matches the requirements of the ISPs determines their actual security behavior. By assessing this match, organizations can adjust the compliance environment for employees, such as the length of time to complete security tasks, to motivate employees to adopt the most appropriate cognitive mode for making compliance judgments to increase the effectiveness of compliance over time. In seeking effective long-term compliance, positive accommodation of environmental elements creates beneficial circumstances for employees in their perceived “comfort zone” for compliance, influencing the organization's overall security posture and culture.

## REFERENCE

- Aggeliki Tsohou, S. K., Maria Karyda, and Kiountouzis, E. 2015. “Managing the Introduction of Information Security Awareness Programmes in Organisations,” *European Journal of Information Systems* (24:1), Taylor & Francis, pp. 38–58. (<https://doi.org/10.1057/ejis.2013.27>).
- Alecse, C. 2023. “The Impact of Choice Overload on Decision Deferral in Cybersecurity,” *The Journal of the Southern Association for Information Systems* (10:2), pp. 1–11.
- Allen, D. 2011. “Information Behavior and Decision Making in Time-constrained Practice: A Dual-processing Perspective,” *Journal of the American Society for Information Science and Technology* (62:11), pp. 2165–2181.
- Allinson, C., and Hayes, J. 2011. *The Cognitive Style Index: Technical Manual and User Guide*, Pearson Education Ltd.
- Allinson, C. W., and Hayes, J. 1996. “The Cognitive Style Index: A Measure of Intuition-Analysis For Organizational Research,” *Journal of Management Studies* (33:1), pp. 119–135. (<https://doi.org/10.1111/j.1467-6486.1996.tb00801.x>).
- Alter, S. 2015. “Beneficial Noncompliance and Detrimental Compliance: Expected Paths to Unintended Consequences,” in *AMCIS 2015, Twenty First Americas Conference on Information Systems, Puerto Rico*.
- Aurigemma, S., and Mattson, T. 2017. “Deterrence and Punishment Experience Impacts on ISP Compliance Attitudes,” *Information & Computer Security* (25:4), pp. 421–436. (<https://doi.org/10.1108/ICS-11-2016-0089>).
- Aurigemma, S., and Mattson, T. 2018. “Exploring the Effect of Uncertainty Avoidance on Taking Voluntary Protective Security Actions,” *Computers & Security* (73), pp. 219–234. (<https://doi.org/10.1016/j.cose.2017.11.001>).
- Aurigemma, S., and Mattson, T. 2019. “Generally Speaking, Context Matters: Making the Case for a Change from Universal to Particular ISP Research,” *Journal of the Association for Information Systems* (20:12), p. 7.
- Belanger, F., Collignon, S., Enget, K., and Negangard, E. 2017. “Determinants of Early Conformance with Information Security Policies,” *Information & Management* (54:7),

- pp. 887–901. (<https://doi.org/10.1016/j.im.2017.01.003>).
- Bélanger, F., Maier, J., and Maier, M. 2022. “A Longitudinal Study on Improving Employee Information Protective Knowledge and Behaviors,” *Computers & Security* (116), p. 102641. (<https://doi.org/10.1016/j.cose.2022.102641>).
- Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. “What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors,” *MIS Quarterly* (39:4), pp. 837–864. (<https://doi.org/10.25300/MISQ/2015/39.4.5>).
- Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J., and Courtney, J. F. 2018. “Intentions to Comply Versus Intentions to Protect: A VIE Theory Approach to Understanding the Influence of Insiders’ Awareness of Organizational SETA Efforts: Intentions to Comply Versus Intentions to Protect,” *Decision Sciences* (49:6), pp. 1187–1228. (<https://doi.org/10.1111/deci.12304>).
- Burns, A. J., Roberts, T. L., Posey, C., Lowry, P. B., and Fuller, B. 2023. “Going Beyond Deterrence: A Middle-Range Theory of Motives and Controls for Insider Computer Abuse,” *Information Systems Research* (34:1), pp. 342–362. (<https://doi.org/10.1287/isre.2022.1133>).
- Butavicius, M., Taib, R., and Han, S. J. 2022. “Why People Keep Falling for Phishing Scams: The Effects of Time Pressure and Deception Cues on the Detection of Phishing Emails,” *Computers & Security* (123), p. 102937. (<https://doi.org/10.1016/j.cose.2022.102937>).
- Changes in Employees’ Job Characteristics During an Enterprise System Implementation: A Latent Growth Modeling Perspective*. 2024.
- Conlon, D., Raeburn, T., and Wand, T. 2023. “Cognitive Continuum Theory: Can It Contribute to the Examination of Confidentiality and Risk-actuated Disclosure Decisions of Nurses Practising in Mental Health?,” *Nursing Inquiry* (30:2), p. e12520. (<https://doi.org/10.1111/nin.12520>).
- Cram, W. A., and D’Arcy, J. 2023. “‘What a Waste of Time’: An Examination of Cybersecurity Legitimacy,” *Information Systems Journal* (33:6), pp. 1396–1422. (<https://doi.org/10.1111/isj.12460>).
- Cram, W. A., D’Arcy, J., and Benlian, A. 2024. “Time Will Tell: The Case for an Idiographic Approach to Behavioral Cybersecurity Research,” *MIS Quarterly* (48:1).
- Cram, W. A., Proudfoot, J. G., and D’Arcy, J. 2017. “Organizational Information Security Policies: A Review and Research Framework,” *European Journal of Information Systems* (26:6), pp. 605–641. (<https://doi.org/10.1057/s41303-017-0059-9>).
- Cram, W. A., Proudfoot, J. G., and D’Arcy, J. 2021. “When Enough Is Enough: Investigating the Antecedents and Consequences of Information Security Fatigue,” *Information Systems Journal* (31:4), Wiley Online Library, pp. 521–549.
- 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. (<https://doi.org/10.2753/MIS0742-122310210>).
- D’Arcy, J., Hovav, A., and Galletta, D. 2009. “User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach,” *Information Systems Research* (20:1), pp. 79–98. (<https://doi.org/10.1287/isre.1070.0160>).
- 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. (<https://doi.org/10.1111/isj.12173>).
- 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. (<https://doi.org/10.1016/j.im.2019.02.006>).
- Dennis, A. R., and Minas, R. K. 2018. “Security on Autopilot: Why Current Security Theories Hijack Our Thinking and Lead Us Astray,” *SIGMIS Database* (49:SI), New York, NY, USA: Association for Computing Machinery, pp. 15–38. (<https://doi.org/10.1145/3210530.3210533>).
- Dhami, M. K., and Mumpower, J. L. 2018. “Kenneth R. Hammond’s Contributions to the Study of Judgment and Decision Making,” *Judgment and Decision Making* (13:1), pp. 1–22. (<https://doi.org/10.1017/S1930297500008780>).
- Dhami, M. K., and Thomson, M. E. 2012. “On the Relevance of Cognitive Continuum Theory and Quasirationality for Understanding Management Judgment and Decision Making,” *European Management Journal* (30:4), pp. 316–326. (<https://doi.org/10.1016/j.emj.2012.02.002>).
- Diestre, L., Barber IV, B., and Santaló, J. 2020. “The Friday Effect: Firm Lobbying, the Timing of Drug Safety Alerts, and Drug Side Effects,” *Management Science* (66:8), INFORMS, pp. 3677–3698.
- Dunwoody, P. T., Haarbauer, E., Mahan, R. P., Marino, C., and Tang, C.-C. 2000. “Cognitive Adaptation and Its Consequences: A Test of Cognitive Continuum Theory,” *Journal of Behavioral Decision Making* (13:1), Wiley Online Library, pp. 35–54.
- Evans, J. S. B., and Stanovich, K. E. 2013. “Dual-Process Theories of Higher Cognition: Advancing the Debate,” *Perspectives on Psychological Science* (8:3), Sage Publications Sage CA: Los Angeles, CA, pp. 223–241.
- Fisher, C. D., and To, M. L. 2012. “Using Experience Sampling Methodology in Organizational Behavior,” *Journal of Organizational Behavior* (33:7), Wiley Online Library, pp. 865–877.
- Frank, M., and Kohn, V. 2023. “Understanding Extra-Role Security Behaviors: An Integration of Self-Determination Theory and Construal Level Theory,” *Computers & Security* (132), p. 103386. (<https://doi.org/10.1016/j.cose.2023.103386>).
- Hammond, K. R. 1980. *The Integration of Research in Judgment and Decision Theory*, (Vol. 226), Center for Research on Judgement and Policy.
- Hammond, K. R. 1981. *Principles of Organization in Intuitive and Analytical Cognition*, Defense Technical Information Center Ft. Belvoir, VA.
- Hammond, K. R. 1996. *Human Judgment and Social Policy: Irreducible Uncertainty, Inevitable Error, Unavoidable Injustice*, Oxford University Press, USA.
- Hammond, K. R. 2010. “Intuition, No! ...Quasirationality, Yes!,” *Psychological Inquiry* (21:4), pp. 327–337. (<https://doi.org/10.1080/1047840X.2010.521483>).
- Hammond, K. R., Hamm, R. M., Grassia, J., and Pearson, T. 1987. “Direct Comparison of the Efficacy of Intuitive and Analytical Cognition in Expert Judgment,” *IEEE Transactions on Systems, Man, and Cybernetics* (17:5), pp. 753–770. (<https://doi.org/10.1109/TSMC.1987.6499282>).
- Hengstler, S., Kuehnel, S., Masuch, K., Nastjuk, I., and Trang, S. 2023a. “Should i Really Do That? Using Quantile Regression to Examine the Impact of Sanctions on Information Security Policy Compliance Behavior,” *Computers & Security* (133), p. 103370.

- (<https://doi.org/10.1016/j.cose.2023.103370>).
- Hengstler, S., Kuehnel, S., Masuch, K., Nastjuk, I., and Trang, S. 2023b. “Should i Really Do That? Using Quantile Regression to Examine the Impact of Sanctions on Information Security Policy Compliance Behavior,” *Computers & Security* (133), p. 103370. (<https://doi.org/10.1016/j.cose.2023.103370>).
- Hu, S., Hsu, C., and Zhou, Z. 2021a. “The Impact of SETA Event Attributes on Employees’ Security-Related Intentions: An Event System Theory Perspective,” *Computers & Security* (109), p. 102404. (<https://doi.org/10.1016/j.cose.2021.102404>).
- Hu, S., Hsu, C., and Zhou, Z. 2021b. “The Impact of SETA Event Attributes on Employees’ Security-Related Intentions: An Event System Theory Perspective,” *Computers & Security* (109), p. 102404. (<https://doi.org/10.1016/j.cose.2021.102404>).
- Ifinedo, P. 2014. “Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialisation, Influence, and Cognition,” *Information & Management* (51:1), pp. 69–79. (<https://doi.org/10.1016/j.im.2013.10.001>).
- Johnston, A. C., Gangi, P. M. D., Bélanger, F., Crossler, R. E., Siponen, M., Warkentin, M., and Singh, T. 2023. “Seeking Rhetorical Validity in Fear Appeal Research: An Application of Rhetorical Theory,” *Computers & Security* (125), p. 103020. (<https://doi.org/10.1016/j.cose.2022.103020>).
- Johnston, A. C., Warkentin, M., and Siponen, M. 2015. “An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric,” *MIS Quarterly* (39:1), pp. 113–134. (<https://doi.org/10.25300/MISQ/2015/39.1.06>).
- 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. (<https://doi.org/10.1287/isre.2018.0827>).
- Karjalainen, M., Siponen, M., and Sarker, S. 2020. “Toward a Stage Theory of the Development of Employees’ Information Security Behavior,” *Computers & Security* (93), p. 101782. (<https://doi.org/10.1016/j.cose.2020.101782>).
- Kim, S. S., and Kim, Y. J. 2017. “The Effect of Compliance Knowledge and Compliance Support Systems on Information Security Compliance Behavior,” *Journal of Knowledge Management* (21:4), pp. 986–1010. (<https://doi.org/10.1108/JKM-08-2016-0353>).
- Kyngas, H., Hentinen, M., Koivukangas, P., and Ohinmaa, A. 1996. “Young Diabetics’ Compliance in the Framework of the MIMIC Model,” *Journal of Advanced Nursing* (24:5), Wiley Online Library, pp. 997–1005.
- Li, H., Luo, X. (Robert), and Chen, Y. 2021. “Understanding Information Security Policy Violation from a Situational Action Perspective,” *Journal of the Association for Information Systems* (22:3), pp. 739–772. (<https://doi.org/10.17705/1jais.00678>).
- Lipshitz, R., and Strauss, O. 1997. “Coping with Uncertainty: A Naturalistic Decision-Making Analysis,” *Organizational Behavior and Human Decision Processes* (69:2), Elsevier, pp. 149–163.
- Liu, C., Wang, N., and Liang, H. 2020. “Motivating Information Security Policy Compliance: The Critical Role of Supervisor-Subordinate Guanxi and Organizational Commitment,” *International Journal of Information Management* (54), p. 102152. (<https://doi.org/10.1016/j.ijinfomgt.2020.102152>).
- Newell, B. R., and Shanks, D. R. 2014. “Unconscious Influences on Decision Making: A Critical Review,” *Behavioral and Brain Sciences* (37:1), Cambridge University Press, pp. 1–19.

- Nobles, C. 2022. "Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem," *HOLISTICA: Journal of Business & Public Administration* (13:1), pp. 49–72.
- O'Connor, T., Gibson, J., Lewis, J., Strickland, K., and Paterson, C. 2023. "Decision-Making in Nursing Research and Practice—Application of the Cognitive Continuum Theory: A Meta-Aggregative Systematic Review," *Journal of Clinical Nursing*, Wiley Online Library.
- Paananen, H., Lapke, M., and Siponen, M. 2020. "State of the Art in Information Security Policy Development," *Computers & Security* (88), p. 101608. (<https://doi.org/10.1016/j.cose.2019.101608>).
- Rieger, A., Roth, T., Sedlmeir, J., Fridgen, G., and Young, A. 2024. "Organizational Identity Management Policies," *Journal of the Association for Information Systems* (25:3), pp. 522–527.
- Safa, N. S., Solms, R. V., and Furnell, S. 2016. "Information Security Policy Compliance Model in Organizations," *Computers & Security* (56), pp. 70–82. (<https://doi.org/10.1016/j.cose.2015.10.006>).
- Sarkar, S., Vance, A., Ramesh, B., Demestihis, M., and Wu, D. T. 2020. "The Influence of Professional Subculture on Information Security Policy Violations: A Field Study in a Healthcare Context," *Information Systems Research* (31:4), pp. 1240–1259. (<https://doi.org/10.1287/isre.2020.0941>).
- Serva, M. A., Kher, H., and Laurenceau, J.-P. 2011. "Using Latent Growth Modeling to Understand Longitudinal Effects in MIS Theory: A Primer," *Communications of the Association for Information Systems* (28). (<https://doi.org/10.17705/1CAIS.02814>).
- Siponen, M., and Iivari, J. 2006. "IS Security Design Theory Framework and Six Approaches to the Application of ISPs and Guidelines," *Journal of the Association for Information Systems* (7:7), pp. 445–472.
- Slovic, P., Finucane, M. L., Peters, E., and MacGregor, D. G. 2004. "Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality," *Risk Analysis* (24:2), pp. 311–322. (<https://doi.org/10.1111/j.0272-4332.2004.00433.x>).
- Standing, M. 2008. "Clinical Judgement and Decision-Making in Nursing—Nine Modes of Practice in a Revised Cognitive Continuum," *Journal of Advanced Nursing* (62:1), Wiley Online Library, pp. 124–134.
- Tsohou, A., Karyda, M., and Kokolakis, S. 2015. "Analyzing the Role of Cognitive and Cultural Biases in the Internalization of Information Security Policies: Recommendations for Information Security Awareness Programs," *Computers & Security* (52), pp. 128–141. (<https://doi.org/10.1016/j.cose.2015.04.006>).
- Tyler, T. R., and Blader, S. L. 2005. "Can Businesses Effectively Regulate Employee Conduct? The Antecedents of Rule Following in Work Settings," *Academy of Management Journal* (48:6), pp. 1143–1158. (<https://doi.org/10.5465/amj.2005.19573114>).
- Vance, A., Eargle, D., Eggett, D., Straub, D., and Ouimet, K. 2022. "Do Security Fear Appeals Work When They Interrupt Tasks? A Multi-Method Examination of Password Strength," *MIS Quarterly* (45:3), pp. 1721–1738. (<https://doi.org/10.25300/MISQ/2022/15511>).
- Vance, A., Jenkins, J. L., Anderson, B. B., Bjornn, D. K., and Kirwan, C. B. 2018. "Tuning Out Security Warnings: A Longitudinal Examination of Habituation Through fMRI, Eye Tracking, and Field Experiments," *MIS Quarterly* (42:2), pp. 355–380. (<https://doi.org/10.25300/MISQ/2018/14124>).
- Vance, A., Siponen, M., and Pahnla, S. 2012. "Motivating IS Security Compliance: Insights

- from Habit and Protection Motivation Theory,” *Information & Management* (49:3–4), pp. 190–198. (<https://doi.org/10.1016/j.im.2012.04.002>).
- Vance, A., Siponen, M. T., and Straub, D. W. 2020. “Effects of Sanctions, Moral Beliefs, and Neutralization on Information Security Policy Violations across Cultures,” *Information & Management* (57:4), p. 103212. (<https://doi.org/10.1016/j.im.2019.103212>).
- Venkatesh, V., Davis, F. D., and Zhu, Y. 2023. “Competing Roles of Intention and Habit in Predicting Behavior: A Comprehensive Literature Review, Synthesis, and Longitudinal Field Study,” *International Journal of Information Management* (71), p. 102644. (<https://doi.org/10.1016/j.ijinfomgt.2023.102644>).
- Wang, J., Gupta, M., and Rao, H. R. 2015. “Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications,” *MIS Quarterly* (39:1), pp. 91–112. (<https://doi.org/10.25300/MISQ/2015/39.1.05>).
- Warkentin, M., Johnston, A. C., Shropshire, J., and Barnett, W. D. 2016a. “Continuance of Protective Security Behavior: A Longitudinal Study,” *Decision Support Systems* (92), pp. 25–35. (<https://doi.org/10.1016/j.dss.2016.09.013>).
- Warkentin, M., Johnston, A. C., Shropshire, J., and Barnett, W. D. 2016b. “Continuance of Protective Security Behavior: A Longitudinal Study,” *Decision Support Systems* (92), pp. 25–35. (<https://doi.org/10.1016/j.dss.2016.09.013>).
- Yazdanmehr, A., and Wang, J. 2016. “Employees’ Information Security Policy Compliance: A Norm Activation Perspective,” *Decision Support Systems* (92), pp. 36–46. (<https://doi.org/10.1016/j.dss.2016.09.009>).

## APPENDIX A: LONGITUDINAL STUDIES ON COMPLIANCE WITH INFORMATION SECURITY POLICIES.

Author	Theory	Method	Influenced Factors	Compliance Context	Cognitive Preference
Belanger et al. (2017)	The Theory of Planned Behavior	Survey, 535 participants in a university, 6 months	Organizational triggers, ISP change awareness, perceived threat severity, perceived threat susceptibility, attitude, subjective norm, self-efficacy	Password creation and change	Normatively believing that compliance is right, understanding how and why to comply, and understanding the threats of noncompliance
Belanger et al. (2022)	Protection Motivation Theory	Survey, 826 German employees, 10 months	Knowledge, privacy concern, perceived risk	Passcodes for encryption, Bluetooth use, and location-based information sharing	Understanding the importance of security behavior
Boss et al. (2015)	Protection Motivation Theory	Experiment, 104 and 327 students, 8 weeks	Perceived threat severity, perceived threat vulnerability, response efficacy, self-efficacy, response costs, fear	Data backups, anti-malware software use	Understanding how and why to comply, understanding the consequences of noncompliance, and assessing the cost of compliance
Cram & D'Arcy (2023)	Organizational Legitimacy	Survey, 529 Prolific participants, 7 months	Top management support, cybersecurity inconvenience, cybersecurity legitimacy, incident probability	General compliance with ISPs	Normatively believing that compliance is right, understanding the importance of security behavior, and rationally assessing the cost of security incidents
Cram et al. (2024)	Neutralization	ESM, 108 university students, 4 weeks	Neutralization, positive affect, negative affect	General compliance with ISPs	Rationalizing insecurity behavior through neutralization techniques
D'Arcy & The (2019)	Affective Events Theory, Coping Theory	ESM, 138 employees, 3 weeks	Security-related stress, frustration, fatigue, neutralization	General compliance with ISPs	Rationalizing noncompliance through neutralization techniques
D'Arcy & Lowry (2019)	Rational Choice Theory, The Theory of Planned	ESM, 77 MTurk participants, 2 weeks	Positive affect, negative affect, work impediment, benefits of compliance, computer monitoring, moral beliefs, organizational citizenship behavior,	General compliance with ISPs	Normatively believing that compliance is right, understanding how and why to comply, morally willing to



	Behavior		deviance, subjective norms, coworker compliance, self-efficacy, attitude toward compliance		comply, and rationally assessing the benefits and costs of compliance
Hengstler et al. (2023)	Deterrence Theory	Survey, 263 MTurk participants, 30 days	Formal sanction certainty, formal sanction severity, informal sanction certainty, informal sanction severity	General compliance with ISPs	Rationally assessing the benefits and costs of compliance
Warkentin et al. (2016)	Protection Motivation Theory	Experiment, 253 university students, 6 weeks	Perceived threat severity, perceived threat susceptibility, response efficacy, self-efficacy, perceived extraneous circumstances	Anti-malware software use	Regularly using security tools, understanding how and why to comply, and understanding the consequences of noncompliance

**Note:** ESM, Experienced Sampling Method; ISP, Information Security Policy; MTurk, Amazon Mechanical Turk.

## REFERENCE

- Bélanger, F., Collignon, S., Enget, K., and Negangard, E. 2017. “Determinants of Early Conformance with Information Security Policies,” *Information & Management* (54:7), pp. 887–901.
- Bélanger, F., Maier, J., and Maier, M. 2022. “A Longitudinal Study on Improving Employee Information Protective Knowledge and Behaviors,” *Computers & Security* (116), p. 102641.
- Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. “What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors,” *MIS Quarterly* (39:4), pp. 837–864.
- Cram, W. A., and D’Arcy, J. 2023. “‘What a Waste of Time’: An Examination of Cybersecurity Legitimacy,” *Information Systems Journal* (33:6), pp. 1396–1422.
- Cram, W. A., D’Arcy, J., and Benlian, A. 2024. “Time Will Tell: The Case for an Idiographic Approach to Behavioral Cybersecurity Research,” *MIS Quarterly* (48:1).
- 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.
- Hengstler, S., Kuehnel, S., Masuch, K., Nastjuk, I., and Trang, S. 2023. “Should i Really Do That? Using Quantile Regression to Examine the Impact of Sanctions on Information Security Policy Compliance Behavior,” *Computers & Security* (133), p. 103370.
- Warkentin, M., Johnston, A. C., Shropshire, J., and Barnett, W. D. 2016. “Continuance of Protective Security Behavior: A Longitudinal Study,” *Decision Support Systems* (92), pp. 25–35.

## APPENDIX B: REVISED COGNITIVE STYLE INDEX QUESTIONNAIRE (adapted from Allinson & Hayes, 1996)

Employees differ in the way they think about compliance with information security policies (ISPs). Below are 38 statements designed to identify your own approach. If you believe that a statement is true about you, answer “T”. If you believe that it is false about you, answer “F”. If you are uncertain whether it is true or false, answer “?”. This is not a test of your ability, and there are no right or wrong answers. Simply choose the one response which comes closest to your own opinion. Give your first reaction in each case, and make sure that you respond to every statement. Indicate your answer by completely filling in the appropriate oval opposite the statement:

		T	?	F
1.	In my experience, rational thought is the only realistic basis for compliance with ISPs.	2	1	0
2.	To comply with ISPs, I have to study each part of it in detail.	2	1	0
3.	I am most effective when my work involves a clear sequence of the requirements of an ISP to be performed.	2	1	0
4.	I have difficulty working with people who ‘dive in at the deep end’ without considering the finer aspects of compliance with ISPs.	2	1	0
5.	I am careful to follow the requirements of ISPs at work.	2	1	0
6.	I avoid taking a course in compliance with ISPs if the odds are against its success.	2	1	0
7.	I am inclined to scan through ISPs rather than read them in detail.	0	1	2
8.	My understanding of the requirements of an ISP tends to come more from thorough analysis than flashes of insight.	2	1	0
9.	I try to keep a regular routine of complying with ISPs in my work.	2	1	0
10.	The kind of compliance with ISPs I like best is that which requires a logical, step-by-step approach.	2	1	0
11.	I rarely make ‘off the top of the head’ decisions for compliance with ISPs.	2	1	0
12.	I prefer chaotic action to orderly inaction in compliance with ISPs.	0	1	2
13.	Given enough time, I would consider every situation from all angles of compliance with ISPs.	2	1	0
14.	To be successful in compliance with ISPs, I find that it is important to avoid hurting other people’s feelings.	2	1	0
15.	The best way for me to understand the requirements of an ISP is to break them down into their constituent parts.	2	1	0

16.	I find that adopting a careful, analytical approach to making decisions for compliance with ISPs takes too much time.	0	1	2
17.	I make the most progress when I take calculated risks of compliance with ISPs.	0	1	2
18.	I find that it is possible to be too organized when complying with certain kinds of ISPs.	0	1	2
19.	I always pay attention to detail before I reach a decision for compliance with ISPs.	2	1	0
20.	I make many of my decisions for compliance with ISPs on the basis of intuition.	0	1	2
21.	My philosophy is that it is better to be safe than risk being sorry in compliance with ISPs.	2	1	0
22.	When making a decision for compliance with ISPs, I take my time and thoroughly consider all relevant factors.	2	1	0
23.	I get on best with quiet, thoughtful people in compliance with ISPs.	2	1	0
24.	I would rather that my compliance with ISPs was unpredictable than that it followed a regular pattern.	0	1	2
25.	Most people regard me as a logical thinker in compliance with ISPs.	2	1	0
26.	To fully understand the reasons of compliance with ISPs I need a good theory	2	1	0
27.	I work best in compliance with ISPs with people who are spontaneous.	0	1	2
28.	I find detailed, methodical compliance with ISPs satisfying.	2	1	0
29.	My approach to following the requirements of an ISP is to focus on one part at a time.	2	1	0
30.	I am constantly on the lookout for new experiences in compliance with ISPs.	0	1	2
31.	In compliance with ISPs, I have more to say than most.	0	1	2
32.	My 'gut feeling' is just as good a basis for decision-making for compliance with ISPs as careful analysis.	0	1	2
33.	I am the kind of person who casts caution to the wind.	0	1	2
34.	I make decisions for compliance with ISPs and get on with the requirements rather than analyze every last detail.	0	1	2
35.	I am always prepared to take a gamble on compliance with ISPs.	0	1	2
36.	Formal plans for compliance with ISPs are more of a hindrance than a help in my work.	0	1	2
37.	I am more at home with ideas rather than facts and figures in compliance with ISPs.	0	1	2
38.	I find that 'too much analysis results in paralysis' in compliance with ISPs.	0	1	2

## REFERENCE

Allinson, C. W., and Hayes, J. 1996. "The Cognitive Style Index: A Measure of Intuition-Analysis For Organizational Research," *Journal of Management Studies* (33:1), pp. 119–135.