Between Habit and Control – Opening the Black Box of ISP Compliance Under Stress

Theresa Pfaff[1]
Paderborn University,
Paderborn, Germany

Florian Rampold
University of Goettingen
Goettingen, Germany

Gilbert Georg Hoevel
Paderborn University,
Paderborn, Germany

Jana Driller
Paderborn University,
Paderborn, Germany

ABSTRACT

The persistent challenge of ensuring employee adherence to information security policies (ISPs) has long been a central concern for organizations. While much research has focused on rational decision-making processes, the interplay between internal habitual behaviors and external organizational controls remains underexplored. This study delves into the comparative influence of habit—as an ingrained individual trait—and detection certainty—an organizational control mechanism—on ISP compliance. Using a survey-based online experiment, our study intends to expand our knowledge of compliance drivers and effects in stressful working environments. To the best of our knowledge, this study takes initiating effort in subjecting participants to real-time stress in an online vignette, where they are tasked with navigating compliance challenges within a limited time frame. We explore whether habitual behavior (an internal trait) or detection certainty (an external control) compete or complement each other when facing compliance challenges in stressful and non-stressful situations. With this we aim to contribute to the discussion on optimizing internal training and external controls to enhance ISP compliance in high-pressure environments.

Keywords: Compliance Behavior, Information Security Policies, Stress, Organizational Controls, ISP Compliance, Habit.

[1] Corresponding author. theresa.pfaff@uni-paderborn.de

INTRODUCTION

Human error remains a critical vulnerability in organizational information security (Warkentin et al. 2004). Despite well-crafted ISPs, employees often exhibit non-compliance, driven by factors such as laziness, poor training, or a lack of motivation (D'Arcy and Lowry 2019). Organizations rely on ISPs to mitigate insider threats and guide employee behavior; however, the persistence of insecure practices suggests that compliance cannot be solely understood through a rational, decision-making lens. While the deterrence theory has shown that employee's detection certainty influences their intention to comply (D'Arcy and Herath 2011), the field of information security compliance has often neglected the non-rational, unintentional drivers of behavior. Habit, a well-established psychological construct, plays a critical role in shaping behavior that becomes ingrained over time (Verplanken and Wood 2006), particularly in routinized tasks, such as emailing, where security may not be a conscious focus. Employees' habitual compliance behaviors may significantly influence ISP adherence, but they do so in the shadow of external controls such as detection certainty, which organizations use to enforce ISP compliance. For employees, who already established a compliance habit, external controls may seem obsolete or perhaps even have an adverse effect by conveying the feeling that the organization does not trust its employees' competencies (Frey, 1993). Furthermore, it is questionable whether external controls have an effective effect at all when factors such as time stress are considered. According to Statista (2022), 73% of employees from five different countries reported that their usual stress level is high or moderate at work. This is critical, since research shows that when under stress, individuals process less information and often revert to habitual, automatic behaviors since cognitive resources are impaired during stress perception (Verplanken 1993). Surprisingly, despite its importance, the intersection of time stress and

information security tasks remains largely unexplored. Chowdhury et al. (2019) identified just four studies that examined time pressure in security contexts, with none investigating its role in an actual stressful experimental setting. Therefore, we aim to answer the following research question (RQ)*:*

RQ: How does time stress impact the relationship between habit (an internal trait) and detection certainty (an external control) on ISP compliance ?

By focusing on an online experimental task that exposes participants to real-time stress, we aim to enhance our understanding of ISP compliance drivers and contribute to the optimization of strategies that promote desired behaviors for both organizations and employees.

THEORETICAL BACKGROUND

Deterrence mechanisms are pivotal in influencing ISP compliance, suggesting that individuals avoid non-compliance when they perceive a high likelihood of detection and punishment (Gibbs 1975; Straub 1990). This cost-benefit approach emphasizes external controls—like audits and sanctions—to shape behavior. Of all deterrence mechanisms, studies affirm that detection certainty reduces ISP violations most effectively (D'Arcy et al. 2009). However, Siponen and Vance (2010) note that it addresses intentional non-compliance but neglects unintentional behaviors. Most ISP incidents (e.g. through phishing, social engineering etc.) occur due to stress-related, non-intentional actions (Pahnila et al. 2007). In stressful situations, such as email answering in a rush, automatic behaviors dominate over rational decisions (Verplanken 1993). This leads to a broader consideration of how external organizational factors, such as detection certainty, interact with internal behavioral patterns, especially in environments where employees face time stress and other challenges.

While deterrence theory focuses on external incentives, ISP compliance behaviors may be increasingly influenced by internal processes. Habit, a behavior learned through repetition, shapes employee actions in routine tasks, bypassing conscious decision-making (Verplanken et al. 2003). They form as employees repeatedly follow security protocols, making compliance automatic rather than deliberate (Limayem et al. 2004). Habits are self-reinforcing, less dependent on external cues, and resistant to changes in controls like detection certainty, especially in low-risk tasks (Wood and Neal 2007). Psychological research shows that habits can override rational decision-making, particularly under stress, when automatic responses dominate (Ouellette and Wood 1998). This challenges the effectiveness of deterrence mechanisms, as strong habits can drive compliance even without monitoring, while weak habits may make employees more reliant on external controls. By incorporating habit, we offer a deeper understanding of ISP compliance, especially in stress-related settings.

RESEARCH DESIGN

Organizations rely on ISPs to ensure employees follow secure behaviors. However, simply enacting a policy does not guarantee compliance (Chen et al. 2012). On the employees' side, detection certainty increases the costs of non-compliant behavior, as individuals believe they are more likely to be caught when violating the ISP (Peace et al. 2003). Unlike actions based on rational assessments, habits are routinized, making them less dependent on immediate environmental cues (Aarts and Dijksterhuis 2000). In the context of ISP compliance, habits can form through the repeated enactment of security behaviors. Once ingrained, habitual behaviors are performed automatically, often with minimal cognitive effort (Limayem and Hirt 2003). Therefore, we hypothesize:

H1: Detection certainty has a positive impact on ISP compliance.

H2: Habit has a positive impact on ISP compliance.

According to Lazarus and Folkman (1984), stress arises when the demands of a task exceed an individual's resources available. Time pressure is a specific form of stress that forces individuals to act quickly, often reducing their ability to consider all available information (Suri and Monroe 2003). Studies on phishing vulnerability (Marett and Wright 2009; Wang et al. 2012) have shown that individuals under time pressure are more likely to make security mistakes. Within the ISP compliance context, time stress reduces employees' capacity to deliberate on security behaviors, increasing the likelihood of unintentional violations (D'Arcy et al. 2014). Therefore, we state:

H3: Time stress has a negative impact on ISP compliance.

Under stress, individuals may rely on fast, intuitive decision-making rather than slower, more deliberate processes (Kahneman 2003). In such situations, high detection certainty may create cognitive dissonance: employees are aware of the consequences of non-compliance but lack the time or cognitive resources to fully process this information, leading to reduced compliance. Stress not only impairs rational decision-making but also amplifies reliance on automatic behaviors, including habits. Stress depletes cognitive resources, prompting individuals to revert to previously learned behaviors that require minimal cognitive effort (Groves and Thompson 1970). In the context of ISP compliance, individuals with strong compliance habits may be more likely to maintain adherence under stress, as their behavior is driven by automaticity rather than conscious deliberation (Ouellette and Wood 1998). This leads us to hypothesize that habitual compliance will become even more pronounced under time stress, as employees rely on their established routines. Thus, we propose:

H4a: The positive relationship between detection certainty and ISP compliance is weakened under time stress.

H4b: The positive relationship between habit and ISP compliance is strengthened under time stress.

The proposed research model is illustrated in Figure 1.

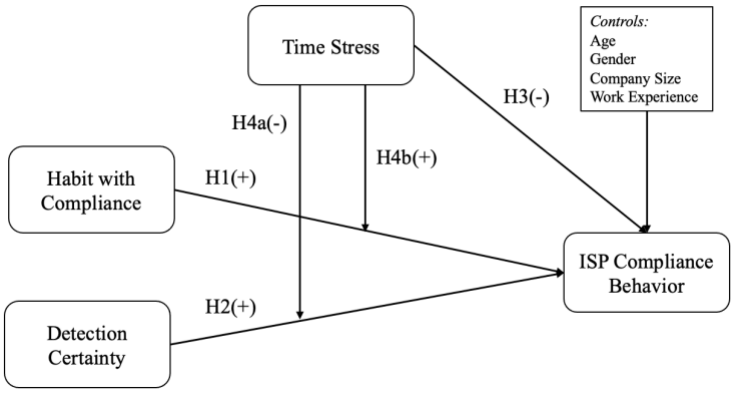

Figure 1. Research Model

METHODOLOGY

Demanding work environments are characterized by variability, unpredictability, and the need for adaptability. Email tasks exemplify these characteristics, requiring quick responses to diverse situations. To make the online experiment as realistic as possible, participants will be presented with eight emails, four of which required actions that violated the ISP, such as sharing internal documents, passwords, or failing to log off properly. This design follows the approach of D'Arcy et al. (2014) and Siponen and Vance (2010). Prior to beginning the task, all participants will be required to read and familiarize themselves with an ISP, which serves as behavioral reference point for the experiment. A sample email will be provided for familiarity with the task and participants can enter a name to feel addressed in the salutation. Time stress will be induced using an eight-minute limit (μ-σ), determined through a pilot study beforehand (n=37), where the average completion time was twelve minutes with a standard deviation of four minutes. With normally distributed data, this requires about 84% of the participants to make faster decisions. In the control group, no time limit will be given. The online experiment follows a between-subjects

design in which participants will be randomly assigned to one of the two treatments. Afterwards, participants will answer a survey with constructs, controls, and demographics, using established scales adapted from literature (Appendix A). For evaluation of ISP compliance, the coding scale as presented in Appendix B will be applied. An exemplary email in the online environment is depicted in Figure 2.

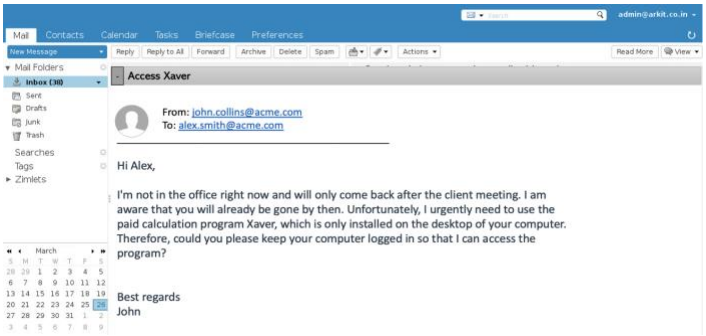

Figure 2. Online Design (Mail 3: Failure to log off)

EXPECTED CONTRIBUTIONS

Our study aims to explore how time stress disrupts ISP compliance, potentially highlighting the limits of deterrence mechanisms. By integrating time stress, we challenge the assumption that external controls effectively ensure adherence in fast-paced environments. If this is the case, organizations should focus on targeted trainings that integrates security into daily routines forming compliance as a habit. Our long-term goal is to develop information security training that equips employees to manage stress and make ISP-conscious decisions effectively, even under pressure.

ACKNOWLEDGEMENTS

This paper has been developed as part of the project “ITS.kompetent” funded by the German Federal Ministry for Economic Affairs and Climate Action (Grant numbers: 01MS20008A and 01MS20008B). We would like to thank the German Federal Ministry for Economic Affairs and Climate Action for the support.

APPENDIX

Appendix A. Survey Items and Email Task

Habit (with Compliance)		**References**
H1	Complying with information security policies is something I do frequently	Verplanken et al. (2003); Vance et al. (2014)
H2	Complying with information security policies is something I do automatically.	
H3	Complying with information security policies is something I do without thinking	
H4	Complying with information security policies is something that belongs to my (daily, weekly, monthly) routine.	
Detection Certainty		Herath and Rao (2009); D'Arcy et al. (2009); Peace et al. (2003); Siponen et al. (2014)
D1	I believe that my organization can detect policy violations effectively.	
D2	There are high chances of being caught if I do not comply with the ISP.	
D3	If I violate the security policy, it is likely that someone will find out.	
D4	I believe that non-compliance with the ISP will be detected.	
Perceived Stress (Control for effective manipulation of time stress)		Suri and Monroe (2003); Wang et al. (2012)
PS1	I felt stressed by the time constraints while performing the task.	
PS3	I felt rushed because of the time limit.	
PS4	The time constraints made the task more challenging.	
Realism (Control for realistic email design)		Johnston et al. (2016)
R1	The presented situations in the mails are realistic.	
R2	I could imagine getting similar mails at work.	
R3	These situations could occur in the workplace.	

ISP Compliance (D'Arcy et al. 2014; Jaeger and Eckhardt 2018; Trang and Nastjuk 2021)			
MAIL1 Sending confidential data to unsecured email address	Hey X, I'm working from home today due to illness and can't access my work emails from here. So, I haven't had a chance to look at the CVs you sent me to fill the new position. Therefore, can you please send me the CVs of our candidates to this mail address? Also, did you already had a look at the application letters? Do you have a preference who to invite to an interview? Just tell me and I will consider it. Thanks! Sarah	**MAIL2** Password sharing	Hello X, I have already left the office for the meeting with our next client and realized that my cloud credentials are not saved on my new laptop. However, I need to log into the server as that is the only place where I have saved the latest version of the presentation. Could you please send me your access data for the data server so that I can download the presentation from the team folder? The presentation starts in 30 minutes. Thank you very much! Eric
MAIL3 Failure to log off	Hi X, I'm not in the office right now and will only come back after the client meeting. I am aware that you will already be gone by then. Unfortunately, I urgently need to use the paid calculation program Xaver, which is only installed on the desktop of your computer. Therefore, could you please keep your computer logged in so that I can access the program? Best regards John	**MAIL4** Copying data to unsecure USB drive	Hey X, Thank you for your help yesterday in preparing the presentation for our client. I just noticed that we only saved the current version on your computer. Could you quickly copy the presentation onto my USB stick and bring it straight to the next client meeting this afternoon? It's right on my desk. Thanks for your help! Susan

Appendix B. Coding Scale for Evaluation

Non-compliant – 0	**Compliant – 1**	**Missing value – N/A**
• Did as requested • Suggested another solution but still did not comply • Stated they would do as requested after approval of the boss	• Did not do as requested • Suggested another solution but still complied • Searched for compliant alternatives	• Evaluation but no indication of action • Answers apart from context • No answer due to elapsed time

REFERENCES

Aarts, H., & Dijksterhuis, A. (2000). Habits as knowledge structures: automaticity in goal-directed behavior. *Journal of personality and social psychology*, *78*(1), 53.

Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach?. *Journal of Management Information Systems*, *29*(3), 157-188.

Chowdhury, N. H., Adam, M. T., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. *Computers & Security*, *97*, 101963.

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the context of information security. *Journal of Information Systems Security*, 7(1), 1-17.

D'Arcy, J., & Lowry, P. B. (2019). Exploring the relationship between organizational culture and compliance with information security policies. *Computers & Security*, 87, 101564.

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., 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.

Frey, B. S. (1993). Does monitoring increase work effort? The rivalry with trust and loyalty. *Economic Inquiry*, *31*(4), 663-670.

Gibbs, J. P. (1975). *Crime, Punishment, and Deterrence*. New York: Elsevier.

Groves, P. M., & Thompson, R. F. (1970). Habituation: a dual-process theory. *Psychological review*, *77*(5), 419.

Herath, T., and Rao, H. R. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.

Jaeger, L., & Eckhardt, A. (2018). When colleagues fail: Examining the role of information security awareness on extra-role security behaviors.

Johnston, A. C., Warkentin, M., and Siponen, M. (2016). "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric," *MIS Quarterly* (40:3), pp. 917-929.

Kahneman, D. (2003). *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux.

Lazarus, R. S., & Folkman, S. (1984). *Stress, Appraisal, and Coping*. New York: Springer.

Limayem, M., & Hirt, S. G. (2003). Force of habit and information systems usage: Theory and initial validation. *Journal of the Association for information Systems*, *4*(1), 3.

Limayem, M., Hirt, S. G., & Cheung, C. M. (2004). How habit limits the predictive power of intention: The case of information systems continuance. *MIS Quarterly*, 28(4), 705-737.

Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems*, *27*(1), 273-303.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS quarterly*, *42*(1), 285-A22.

Ouellette, J. A., & Wood, W. (1998). Habit and intention in everyday life: The multiple processes by which past behavior predicts future behavior. *Psychological bulletin*, *124*(1), 54.

Pahnila, S., Siponen, J., & Mahmood, A. N. (2007). Employees' adherence to information security policies: An empirical study. *Computers & Security*, 26(1), 56-62.

Peace, A. G., Galletta, D. F., and Thong, J. Y. L. (2003). "Software Piracy in the Workplace: A Model and Empirical Test," *Journal of Management Information Systems* (20:1), pp. 153-177.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS quarterly*, 487-502.

Siponen, M., Mahmood, M. A., and Pahnila, S. (2014). "Employees' Adherence to Information Security Policies: An Integrative Model," *Information & Management* (51:2), pp. 217-224.

Statista (2022). Percentage of employees in select countries worldwide who stated their stress level was usually high or moderate in 2022. https://www.statista.com/statistics/1367419/employees-with-high-moderate-stress-levels-worldwide/ (Retrieved in October 2024).

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, 1(3), 255-276.

Suri, R., and Monroe, K. B. (2003). "The Effects of Time Constraints on Consumers' Judgments of Prices and Products," *Journal of Consumer Research* (30:1), pp. 92-104.

Trang, S., & Nastjuk, I. (2021). Examining the role of stress and information security policy design in information security compliance behaviour: An experimental study of in-task behaviour. *Computers & Security*, *104*, 102222.

Vance, A., Lowry, P. B., and Eggett, D. (2014). "Using Accountability to Reduce Access Policy Violations in Information Systems," *Journal of Management Information Systems* (29:4), pp. 263-290.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & management*, *49*(3-4), 190-198.

Verplanken, B. (1993). Habits and information processing: A theoretical analysis. *Journal of Personality and Social Psychology*, 64(5), 778-787.

Verplanken, B., & Orbell, S. (2003). Reflections on past behavior: A self-report index of habit strength. *Journal of Applied Social Psychology*, 33(6), 1313-1330.

Verplanken, B., & Wood, W. (2006). Interventions to break and create consumer habits. *Journal of public policy & marketing*, *25*(1), 90-103.

Verplanken, B., Aarts, H., & van Knippenberg, A. (2003). Habit, information acquisition, and the process of behavior change. *Journal of Personality and Social Psychology*, 84(6), 1023-1034.

Wang, J., Herath, T., Chen, R., and Rao, H. R. (2012). "Phishing Susceptibility: An Investigation into the Processing of a Targeted Spear Phishing Email," *IEEE Transactions on Professional Communication* (55:4), pp. 345-362.

Warkentin, M., Whitman, M., & Harkabi, A. (2004). The role of human error in information security breaches: A psychological perspective. *Computers & Security*, 23(1), 46-59.

Wood, W., & Neal, D. T. (2007). A new look at habits and the habit-goal interface. *Psychological Review*, 114(4), 843-863.