Examining Accounting Employees Information Security Policy Stress: Insights from the Justice and Responsibility Rationalization

Randi Jiang
Seidman College of Business School of Accounting, Grand Valley State University,
Allendale, Michigan, USA

ABSTRACT

Previous research has highlighted various sources of stress that accountants face in their work environment, such as excessive workloads, performance evaluations, and role ambiguity or conflict. This study focuses on a specific type of work-related stress experienced by accountants: information security policy (ISP) stress. While a strong ISP can help prevent information security-related fraud within an organization, the need to comply with these policies adds extra pressure to accountants who are already under considerable stress. This added ISP stress may increase the likelihood of accountants intentionally violating the policy. The study examines how accountants cope with the intention to violate ISPs under such pressure. Specifically, it explores two rationalization mechanisms—displacement of responsibility and diffusion of responsibility—and considers how perceived organizational distributive and procedural justice of the ISP can influence accountants' intention to violate these policies.

Keywords: Information security policy, Work stress, Displacement of responsibility, Diffusion of responsibility, Distributive justice, Procedural justice

INTRODUCTION

Organizations implement information security policies (ISPs) to govern employees' use of information technology (IT) and safeguard digital assets. Non-compliance with these policies increases security risks and vulnerability to cyberattacks (Li et al. 2018). Insider threats accounted for 22% of security incidents in 2021, a 68% increase from 2020, with organizations spending an estimated $15 million annually on insider threats—an increase of 34% over the

previous year (Bassett et al. 2021; Proofpoint 2022). Employee-related missteps contributed to approximately 85% of data breaches (Hancock 2020).

Organizations face various threats, such as unauthorized access that enables data alteration, corruption or theft, failure to maintain backups, and the misuse or theft of computer equipment, all of which can damage an organization's reputation. To mitigate these risks, organizations invest heavily in behavioral security measures, including ISP development, training, and technological updates (Willison and Warkentin 2013). However, such measures impose additional burdens on already overstressed employees, requiring compliance with extensive security regulations (D'Arcy and Teh 2019; Johnston et al. 2019). Consequently, voluntary ISP violations, such as password sharing, insider information leaks, and unauthorized system usage, persist despite organizations' preventive efforts (D'Arcy et al., 2014). ISP stress, stemming from demanding security requirements, significantly influences these violations, particularly among accounting employees (D'Arcy et al. 2014; D'Arcy and Teh 2019).

The increasing prevalence of cybersecurity threats poses substantial challenges for accountants and auditors, who play a critical role in ensuring compliance with ISPs. Accounting professionals are tasked with quantifying the financial impacts of cybersecurity incidents and providing accurate disclosures to stakeholders. Recognizing the growing importance of cybersecurity, the American Institute of Certified Public Accountants (AICPA) has integrated cybersecurity considerations into the Certified Public Accountants (CPA) Evolution Framework. These advancements underscore the urgent need for a deeper understanding of how ISP-related stress influences violation behaviors among accounting employees, as this insight is essential for improving compliance and mitigating risks (Janvrin and Wang 2022; Vien 2021).

LITERATURE REVIEW

From a theoretical perspective, the fraud triangle theory is unique to the accounting intentional fraud realm, which can be extended to examine accounting employees' intentional ISP violation behavior. The three factors that make up the fraud triangle are (1) opportunity, (2) pressure, and (3) rationalization. The opportunity arises for intentional fraud when there is an absence of controls, ineffective controls, or the ability to override controls. Work stress or environmental stress may exert pressure or provide an incentive for employees to commit fraud. Finally, rationalization is an attitude or state of mind that allows an individual to make a conscious decision to use any means to present fraudulent or misrepresented information for personal gain (e.g., asset misappropriations, fraud) (Carcello and Hermanson 2008; Murphy and Dacin 2011). Studies in the accounting literature have found that the three dimensions of the fraud triangle are all critical in explaining the likelihood of fraudulent behavior.

Nevertheless, despite this widespread circulation of the fraud triangle theory, it has also been the subject of considerable debate and criticism in recent years on the equal weights of the three elements in different contexts (Free 2015; Murphy and Free 2015). The fraud triangle suggests that the perpetrator has a non-sharable problem grounded in pressure. When aligned with opportunity and rationalization, an otherwise "good" citizen succumbs to committing fraud, known as the accidental fraudster (Ramamoorti et al. 2009). A predator is better organized and has devised more complex concealment schemes (Kranacher and Riley 2019; Kranacher and Stern 2004). The predator modifies the functional fraud triangle antecedents: pressure and rationalization are unnecessary, and the sole element is opportunity (Dorminey et al. 2010; Lokanan 2015). Therefore, the relative importance of the fraud triangle's three elements depends on the violation's context. This research-in-progress paper does not assume that accounting employees are "predators" but rather "accidental fraudsters" when committing ISP violations.

The key elements associated with accidental fraudsters are pressure and rationalization. Accordingly, this paper posits that pressure and rationalization are critical factors in explaining accountants' intentions to violate ISPs, particularly by considering rationalization as a potential mechanism to explain the effect of pressure on intentional ISP violations among accounting employees.

Information security literature has suggested the importance of employees' cognitive appraisal of stress and their coping strategies, such as rationalization, on their ISP violation intention (D'Arcy et al. 2014; Yazdanmehr et al. 2023). The theoretical foundation for the rationalization construct comes from the moral disengagement theory, which argues that the crucial precondition for managers to act opportunistically is due to the ability to disengage moral responsibility from their action by self-justifying the action to make it compatible with moral standards (Bandura 1990; Bandura 1999). Accounting researchers have noticed the imperative role of the rationalization element of the fraud triangle in the context of accounting behavior research (Chong and Wang 2019; Murphy 2012; Murphy and Dacin 2011; Murphy and Free 2015). For example, concerning rationalizing fraud, Murphy and Dacin (2011) identified the following seven categories of rationalizations as (1) moral justification, by reconstruing an act as being morally worthy, (2) advantageous comparison, by comparing the act to something worse, (3) euphemistic labeling, or using convoluted language to make the act look better than it is, (4) minimize, ignore, or misconstrue the consequences of the act, (5) denial of or blaming the victim, (6) displacing responsibility by blaming someone else, and (7) diffusing responsibility, by blaming everyone else." Specifically, this research concentrates on responsibility rationalization as justification for unethical behavior (i.e., intentional ISP violations) (Chong and Wang 2019).

In this research-in-progress paper, the displacement of responsibility specifically refers to attributing personal responsibility to an authority figure. Individuals use this cognitive mechanism to avoid responsibility by attributing his/her responsibility to an authority figure, such as a manager or superior. The individual can shift the 'feeling' of being 'responsible' or 'accountable' from an autonomous state to an agentic state. This psychological shift results in the individual feeling no responsibility for his or her action because any unfavorable consequence can transfer back to the authority figure (e.g., My boss told me to do it) (Detert et al. 2008). Accounting employees engaging in the displacement of responsibility may argue that they are merely following instructions from their superiors and, therefore, are not accountable for their decisions regarding ISP violations.

In contrast, diffusion of responsibility refers to attributing personal responsibility to others. This mechanism allows an individual to avoid the responsibility of accepting the unfavorable consequences of behaviors by dispersing blame among his or her peers. Consequently, individuals engaging in such diffusion will have little concern for the consequences of their decision, even if it will harm the organization (Mynatt and Sherman 1975). Diffusion of responsibility exists when people believe that the harm associated with an undesirable act is attributed to many people. Therefore, it keeps any one person from feeling personally responsible (Bonner et al. 2016). For example, one easy way to diffuse responsibility is to argue that 'everyone does it!' (McKimmie et al. 2003). Accounting employees engaging in the diffusion of responsibility may feel their obligation is diluted or weakened when their responsibility or blame is perceived to be shared with all other accountants and employees in the organization. Rather than feeling personally responsible, these accounting employees may argue

that they are not at fault because other accountants can also cause the consequence of intentional ISP violations in the organization.

It is anticipated that, when confronted with ISP pressure, accountants will utilize rationalization to justify wrongdoing or unethical behaviors, such as intentional ISP violations (Bies and Shapiro 1987; Snyder 1985; Wood and Mitchell 1981). To further explore the elements of rationalization, perceptions of organizational justice are proposed to influence rationalization as a significant motivational factor contributing to violations of trust against the organization (Rae et al. 2008). This research-in-progress further proposes to examine how the perceived justice of an organization during ISP implementation may serve as a critical factor in determining the target employees choose to hold accountable. Perceived justice will provide situation-based influences on individual cognition and behaviors (Rupp et al. 2014). Therefore, accounting employees can further decide how to rationalize the responsibility for their intentional ISP violations.

Organizational justice research examines various motivators that may lead to employees' perceptions of justice or injustice. Scholars have identified four dimensions of perceived organizational justice – distributive, procedural, informational, and interactional(Colquitt et al. 2001). Previous investigations of negative outcomes of perceived organizational justice have provided theoretical evidence featuring distributive and procedural injustice perceptions as driving motivations for undesirable employee behavior (Colquitt et al. 2001). In contrast, informational and interactional injustice perceptions explain employees' negative behavior after the undesirable action has been taken.

Given that the focal phenomenon of this research-in-progress is intentional ISP violation behavior, the analysis is limited to two types of perceived justice—distributive justice and

procedural justice—to understand potential antecedents to ISP violation behavior better. Distributive justice focuses on whether the allocation of benefits and costs within a group should be proportional to the contributions of group members (Greenberg 1990; Greenberg and Folger 1983). Following the enforcement of ISPs, employees assess whether the increased security of their computers and data justifies the inconvenience or other potential losses associated with ISP compliance. If the inconvenience (disturbs the work of employees and reduces their work efficiency) that the employees perceive is found to be greater than the actual benefits (rewards), then accountants will perceive distributive injustice. This perception will cause employees to blame the organization or managers for unreasonable ISPs (displacement of responsibility), resulting in ISP violations.

In contrast, procedural fairness has been referred to as the judgments about the fairness of the "rules and processes" (Greenberg and Folger 1983) to be objectively designed and applied. In the context of this research-in-progress, the focus is on how individual accounting employees assess whether ISPs are applied consistently to all accounting employees within the organization. If procedures for detecting and punishing ISP violation behaviors do not appear reasonable, then accounting employees may perceive procedural injustice within the organization. This reaction will further cause the accounting employee to use the justification that other employees are not required to follow the ISP to rationalize their violating behaviors.

It is anticipated that low perceived distributive justice will enable accounting employees to adapt to the displacement responsibility. The displacement will place the blame on the organization or manager who causes their ISP pressure, causing employees to rationalize their violating behavior further. In contrast, high perceived procedural justice will deprive the employee of adapting the diffusion responsibility, therefore unable to blame their colleagues who

cause their ISP pressure and further rationalize their violating behavior. Therefore, the second goal of this study is to investigate whether organizational justice will reduce the magnitude of effects of ISP pressure on accounting employees' responsibility rationalization of intentional ISP violations.

Thus, based on the literature presented above, a proposed research model is presented in Figure 1.

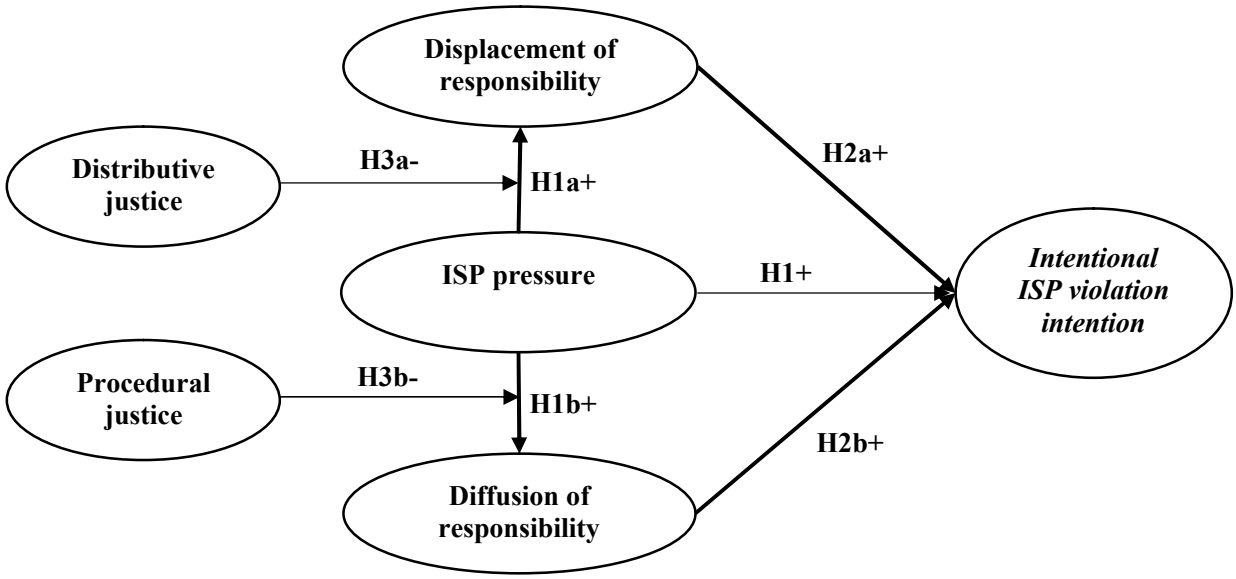

Figure 1. Proposed Research model

PROPOSED METHODOLOGY/CONCLUSION

Information security management controls are integral to an organization's internal control framework, particularly in safeguarding and monitoring sensitive data. Effective IT controls require a multifaceted approach, including understanding the factors that lead accountants to deviate from ISP compliance.

The proposed methodology is to create a multi-study and mixed-method approach involving, if possible, certified public accountants ranging from working in public accounting to

other various industries. We hope this proposed research will contribute to theory and practice by improving our understanding of how accounting employees' perceptions of organizational justice influence their compliance with information security policies.

REFERENCES

Bandura, A. 1990. "Selective Activation and Disengagement of Moral Control," *Journal of Social Issues* (46:1), pp. 27-46.

Bandura, A. 1999. "Moral Disengagement in the Perpetration of Inhumanities," *Personality and Social Psychology Review* (3:3), pp. 193-209.

Bassett, G., Hylender, C. D., Langlois, P., Pinto, A., and Widup, S. 2021. "Data Breach Investigations Report," *Verizon Business*).

Bies, R. J., and Shapiro, D. L. 1987. "Interactional Fairness Judgments: The Influence of Causal Accounts," *Social Justice Research* (1:2), pp. 199-218.

Bonner, J. M., Greenbaum, R. L., and Mayer, D. M. 2016. "My Boss Is Morally Disengaged: The Role of Ethical Leadership in Explaining the Interactive Effect of Supervisor and Employee Moral Disengagement on Employee Behaviors," *Journal of Business Ethics* (137:4), pp. 731-742.

Carcello, J. V., and Hermanson, D. R. 2008. "Fraudulent Financial Reporting: How Do We Close the Knowledge Gap," *Research Studies (White Papers) of Institute for Fraud Prevention (IFP)*).

Chong, V. K., and Wang, I. Z. 2019. "Delegation of Decision Rights and Misreporting: The Roles of Incentive-Based Compensation Schemes and Responsibility Rationalization," *European Accounting Review* (28:2), pp. 275-307.

Colquitt, J. A., Conlon, D. E., Wesson, M. J., Porter, C. O., and Ng, K. Y. 2001. "Justice at the Millennium: A Meta-Analytic Review of 25 Years of Organizational Justice Research," *Journal of applied psychology* (86:3), pp. 425-445.

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 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.

Detert, J. R., Treviño, L. K., and Sweitzer, V. L. 2008. "Moral Disengagement in Ethical Decision Making: A Study of Antecedents and Outcomes," *Journal of Applied Psychology* (93:2), pp. 374-391.

Dorminey, J. W., Fleming, A. S., Kranacher, M.-J., and Riley Jr, R. A. 2010. "Beyond the Fraud Triangle," *The CPA Journal* (80:7), pp. 17-23.

Free, C. 2015. "Looking through the Fraud Triangle: A Review and Call for New Directions," *Meditari Accountancy Research*), pp. 175-196.

Greenberg, J. 1990. "Organizational Justice: Yesterday, Today, and Tomorrow," *Journal of management* (16:2), pp. 399-432.

Greenberg, J., and Folger, R. 1983. "Procedural Justice, Participation, and the Fair Process Effect in Groups and Organizations," in *Basic Group Processes*. Springer, pp. 235-256.
Hancock, J. 2020. "The Psychology of Human Error: Understand the Mistakes That Compromise Your Company's Cybersecurity," *Tessian Research*).
Janvrin, D. J., and Wang, T. 2022. "Linking Cybersecurity and Accounting: An Event, Impact, Response Framework," *Accounting Horizons* (36:4), pp. 67-112.
Johnston, A. C., Warkentin, M., Dennis, A. R., and Siponen, M. 2019. "Speak Their Language: Designing Effective Messages to Improve Employees' Information Security Decision Making," *Decision Sciences* (50:2), pp. 245-284.
Kranacher, M.-J., and Riley, R. 2019. *Forensic Accounting and Fraud Examination*. John Wiley & Sons.
Kranacher, M.-J., and Stern, L. 2004. "Enhancing Fraud Detection through Education," *The CPA journal* (74:11), pp. 66-67.
Li, H., Luo, X. R., Zhang, J., and Sarathy, R. 2018. "Self-Control, Organizational Context, and Rational Choice in Internet Abuses at Work," *Information & Management* (55:3), pp. 358-367.
Lokanan, M. E. 2015. "Challenges to the Fraud Triangle: Questions on Its Usefulness," *Accounting Forum* (39:3), pp. 201-224.
McKimmie, B. M., Terry, D. J., Hogg, M. A., Manstead, A. S., Spears, R., and Doosje, B. 2003. "I'm a Hypocrite, but So Is Everyone Else: Group Support and the Reduction of Cognitive Dissonance," *Group Dynamics: Theory, research, and practice* (7:3), pp. 214-224.
Murphy, P. R. 2012. "Attitude, Machiavellianism and the Rationalization of Misreporting," *Accounting, Organizations and Society* (37:4), pp. 242-259.
Murphy, P. R., and Dacin, M. T. 2011. "Psychological Pathways to Fraud: Understanding and Preventing Fraud in Organizations," *Journal of business ethics* (101:4), pp. 601-618.
Murphy, P. R., and Free, C. 2015. "Broadening the Fraud Triangle: Instrumental Climate and Fraud," *Behavioral Research in Accounting* (28:1), pp. 41-56.
Mynatt, C., and Sherman, S. J. 1975. "Responsibility Attribution in Groups and Individuals: A Direct Test of the Diffusion of Responsibility Hypothesis," *Journal of Personality and Social Psychology* (32:6), pp. 1111-1118.
Proofpoint. 2022. "Ponemon Cost of Insider Threats: Global Report." from https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats
Rae, K., Subramaniam, N., and Sands, J. 2008. "Risk Management and Ethical Environment: Effects on Internal Audit and Accounting Control Procedures," *Journal of Applied Management Accounting Research* (6:1), pp. 11-30.
Ramamoorti, S., Morrison, D., and Koletar, J. W. 2009. "Bringing Freud to Fraud: Understanding the State-of-Mind of the C-Level Suite/White Collar Offender through "Abc" Analysis," *Institute for Fraud Prevention (IFP) at West Virginia University*).
Rupp, D. E., Shao, R., Jones, K. S., and Liao, H. 2014. "The Utility of a Multifoci Approach to the Study of Organizational Justice: A Meta-Analytic Investigation into the Consideration of Normative Rules, Moral Accountability, Bandwidth-Fidelity, and Social Exchange," *Organizational Behavior and Human Decision Processes* (123:2), pp. 159-185.
Snyder, C. R. 1985. "The Excuse: An Amazing Grace," in *The Self and Social Life,* B.R. Schlenker (ed.). pp. 235-260.

Vien, C. 2021. "Wanted: More Systems and Analytics Training for Accounting Students," *Journal of Accountancy* (12).
Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS quarterly*), pp. 1-20.
Wood, R. E., and Mitchell, T. R. 1981. "Manager Behavior in a Social Context: The Impact of Impression Management on Attributions and Disciplinary Actions," *Organizational behavior and human performance* (28:3), pp. 356-378.
Yazdanmehr, A., Li, Y., and Wang, J. 2023. "Employee Responses to Information Security Related Stress: Coping and Violation Intention," *Information Systems Journal* (33:3), pp. 598-639.