Winter 12-10-2023

Information Security Policy Violations in the Work-From-Home Era

Balagopal N
Indian Institute of Technology Madras, ms21d023@smail.iitm.ac.in

Saji K. Mathew
Indian Institute of Technology Madras

Information Security Policy Violations in the Work-From-Home Era

Balagopal N[1]
Department of Management Studies
Indian Institute of Technology Madras
Chennai, Tamil Nadu, India

Saji K Mathew
Department of Management Studies
Indian Institute of Technology Madras
Chennai, Tamil Nadu, India

ABSTRACT

Remote working has become the new normal in modern organizations. This transition has brought various challenges for the organizations in terms of their security infrastructure. Insider threats in organizations have been increasing in recent years. This paper proposes various behavioral and situational aspects that can influence employees' intentions to violate information security policies (ISP) in a remote working environment, including subjective norms, the absence of peer monitoring, and the moderating role of shame. This research also proposes the role of neutralization techniques utilized by employees to rationalize and justify their behavior in the context of policy violations. A conceptual model has been developed, and a pilot study was conducted among 30 participants. This paper contributes to the body of knowledge on ISP compliance in the era of remote working, characterized by behavioral changes of employees.

Keywords: Information Security Policy Violation, Remote Working, Insider Threats, Neutralization, Peer Monitoring, Shame

INTRODUCTION

Over the span of the previous two years, the occurrence of insider threats has witnessed nearly a twofold increase (Ponemon 2022). The IBM Security X-Force Insider Threat Report (IBM 2021) revealed that 40% of cybersecurity incidents involving threats were perpetrated by insiders who had privileged access to companies' information systems. This privileged access

[1] Corresponding Author. ms21d023@smail.iitm.ac.in +91 9746664970

significantly facilitated malicious actions in every confirmed incident involving an insider. The increase in insider incidents has led organizations to develop strategies and allocate resources to protect assets. What factors have contributed to increasing insider threats? What are the remedies? These questions have both practical and theoretical implications.

COVID-19 pandemic has transformed the conventional office work environment into a new normal of remote work, and companies had to adapt to this environment. Even though some organizations had remote working practices to a limited extent, implementing technology across the workforce became difficult. This workplace shift has introduced more unique vulnerabilities that emerge when employees work outside the office environment (Ponemon 2022).

An organization's ISP provides a set of guidelines and procedures that organizations require employees to follow in order to ensure security activities and proper use of organizational information and technology assets (Lowry and Moody 2020). When an employee violates the ISP intentionally or unintentionally, maliciously or non-maliciously, it introduces a threat to the organization's information system (Ponemon 2022). Several prior studies have explored antecedents of employees' deviant behavior from organizations' security policies. However, as the workforce increasingly embraces remote work arrangements, a new context of the work environment is created. There is a paucity of studies addressing the new threats and risks of ISP violation in the context of work-from-home practice (INSA 2021; Li et al. 2022).

In sum, most literature on compliance or non-compliance with ISPs has primarily concentrated on the traditional office work setting. Analyzing the remote work environment will provide valuable insights into the factors that drive security policy violations. This work-in-progress paper aims to investigate ISP violations in the context of work-from-home / remote environments. This study seeks to explore the behavioral factors that motivate employees to

deviate from the established policies in a remote working environment. Ultimately, this research aims to contribute to the body of knowledge surrounding ISPs in the evolving landscape of remote work and assist organizations in safeguarding their infrastructure and digital assets.

LITERATURE REVIEW AND THEORETICAL BACKGROUND

The literature on information security provides diverse explanations regarding various antecedents that influence an employee's intention to violate information security policies. Several studies have utilized the Theory of Neutralization (Sykes and Matza 1957) to understand the effects of various neutralization techniques on ISP violations (Al-Mukahal and Alshare 2015; Barlow et al. 2015; Gwebu et al. 2020; Siponen and Vance 2010; Trinkle et al. 2021; Vance et al. 2021). Siponen and Vance (2010) applied the Neutralization theory to the IS context and their findings indicated that Neutralization is a significant predictor of employees' ISP violation intentions. In their study, Gwebu et al. (2020) examined the impact of beliefs and neutralization on noncompliance behavior and reported that neutralization plays a crucial role as a moderator in the relationship between beliefs and non-compliance. Even under extreme boundary conditions, some employees may seek to rationalize their unethical behavior by denying responsibility for their actions (Trinkle et al. 2021).

Subjective norms play a critical role in ISP compliance behavior. Subjective norms are normative stimuli, beliefs and motivations to comply with a particular act, which is largely informed by consultation or observation of the behaviors of others (Ajzen 1991). In the context of IS security, Bulgurcu et al. (2010) define subjective norms as "an employee's perceived social pressure[s] about compliance with the requirements of the ISP caused by behavioral expectations of such important referents as executives, colleagues, and managers". Employees will be more

inclined to adhere to the policies if they observe that their superiors, peers, and subordinates also comply and follow the guidelines (Chan et al. 2005; Johnston and Warkentin 2010).

The information security literature offers diverse explanations on how social influence can impact employees' adherence to or violations of ISPs (Cheng et al. 2013; D'Arcy and Lowry 2019). Peer monitoring has the potential to impact compliance with ISPs by creating an anticipation that adhering to ISPs aligns with the thoughts and expectations of others. Peer monitoring involves three primary actions: peer noticing, peer correcting, and peer reporting (Yazdanmehr and Wang 2021). In a traditional office work environment, the employee usually notices the behavior of their colleagues. If any employee deviates from acceptable behavior, their peers may either address and correct the behavior or report it to higher authorities. In this way, peer monitoring can serve as an implicit coordination mechanism to encourage and reinforce appropriate behaviors related to ISP.

Information security research has studied the impact of informal controls such as shame, social influence, and moral beliefs on ISP compliance. The role of shame as a mediator between neutralization techniques and the intention to violate security policies was examined in the study conducted by (Silic et al. 2017). Shame has been considered as a possible affective response that employees experience when they violate ISP policy (Farshadkhah et al. 2021).

HYPOTHESIS DEVELOPMENT

Peer Monitoring

When employees notice a policy violation, they are inclined to report it when they are encouraged to do so and when there is an established anonymous reporting procedure (Yazdanmehr and Wang 2021). This helps the organization to enhance its information security posture (Lowry et al. 2013). When an employee works remotely, the absence of peer monitoring

gives her/ him a feeling of being less observed or judged by their colleagues, which can lower the perceived social norm for compliance. We hypothesize that when employees know that their actions are being observed by their peers, it acts as a deterrent against policy violations and reduces the intention to engage in behaviors that would violate the ISP.

H1: Peer monitoring negatively affects employees' intention to violate ISP

Neutralization Techniques

The Theory of Neutralization provides insights into how employees justify their deviant behaviors and alleviate any feelings of guilt or wrongdoing through psychological mechanisms. By employing neutralization techniques, individuals may convince themselves that their actions are justified or necessary under certain circumstances. We argue that remote working provides employees with a greater opportunity to rationalize their behavior. We consider the six dimensions of neutralization from (Siponen and Vance 2010) to test the impact of neutralization techniques on ISP violation intention in the remote working context. Denial of Responsibility (Sykes and Matza 1957) occurs when an employee who engages in deviant behavior acquits oneself of responsibility for their actions. While working remotely, an employee could shift the blame onto external factors such as a lack of immediate IT support. Denial of Injury (Sykes and Matza 1957) occurs when an employee rationalizes an action by downplaying the extent of its negative. An employee who is working out of the office could use her/his personal laptop for processing work-related sensitive data, convincing oneself that the personal device is well-protected and poses no significant risk to the confidentiality or integrity of the data. In Metaphor of the Ledger dimension (Klockars 1974), employees justify their behavior by adopting the notion of compensating bad acts with good acts. An employee who believes that her/his past achievements and positive performance have resulted in an abundance of trust and goodwill from

the organization could rationalize that, occasional violations of ISP while working remotely could be compensated with such past achievements. Defense of Necessity (Minor 1981) involves an employee's rationale that if breaking the rules is perceived as essential, there should be no sense of guilt associated with carrying out the action. The employee can blame the technical difficulties or limitations in remote access that motivated the violation of policy in order to meet a pressing deadline or fulfil a critical task as there was no other option. Condemnation of the Condemners (Sykes and Matza 1957) involves a condition where an employee finds oneself in a moral predicament that necessitates resolving it by violating the law or policy. The employee could justify such actions by blaming the remote working policies that the organization has enforced as unreasonable. In the appeal to higher loyalties dimension (Sykes and Matza 1957), employees hold the belief that their actions contribute to a greater purpose or serve a noble cause, thereby reducing the perceived wrongdoing associated with their deviant behaviors. When working in a remote environment without direct supervision, an employee could prioritize personal relationships and moral obligations over strict adherence to ISPs.

H2: Neutralization techniques positively affect the employees' intention to violate ISP.

Subjective Norms

Subjective norms refer to the perceived social pressure to engage or refrain from a particular behavior. It reflects an individual's belief about what others think one should or should not do in a given situation. In the context of ISPs, subjective norms refer to an employee's perception of the social pressure or expectations surrounding compliance with those established policies within one's work environment. If an employee believes that her/his organization or co-workers place a high value on following these policies, it strengthens the subjective norm for

compliance. The influence of subjective norms works by establishing a normative belief that violating ISP is undesirable and socially unacceptable.

H3. Subjective norms negatively affect employees' intention to violate ISP.

Shame

Shame works as a form of self-imposed sanction and is closely associated with the concept of social norms (Vance et al. 2020). Employees' shame may intensify their perception of social pressure and the importance of conforming to the norms, leading to a decreased intention to violate ISPs. In remote work situations, employees perceive a lower likelihood of being noticed by their peers, resulting in reduced anticipation of potential shame associated with their actions. If an employee does not experience guilt for engaging in deviant behavior, she/he will not feel shame upon others realizing that behavior. We hypothesize that shame has the potential to influence subjective norms, consequently impacting an employee's ISP violation intention.

H4. The relationship between subjective norms and employees' intention to violate ISP is positively moderated by shame such that the relationship is stronger for employees who experience a higher level of shame.

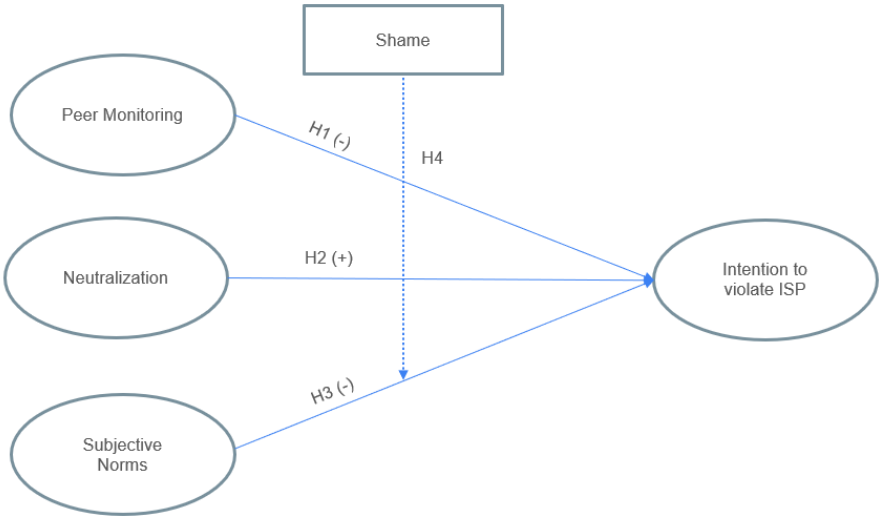

Figure 1. Proposed Research Model

RESEARCH DESIGN

We propose to measure the constructs of Peer monitoring, Neutralization, Subjective norms and Shame through a hypothetical scenario method. Here, the participants will be presented with an ISP violation scenario, and subsequently, they will be asked to respond to the questions regarding the probability of engaging in similar behavior given the same situations. For the constructs in the research model, items have been drawn from the previous ISP studies (Yazdanmehr and Wang 2021; Johnson and Warkentin 2010; Siponen and Vance 2010). We conducted a pilot study with a sample of 30 Executive MBA students in a premier engineering institute in India, who were familiar with Information Security and had an industrial experience of at least four years. The pilot study was used to validate items of existing constructs.

CONCLUSION AND FUTURE WORK

In today's digital landscape, addressing insider threats and ISP violations arising due to the unique challenges in the context of remote working is critically important. This paper synthesized a conceptual model from relevant prior theories to explain ISP violation in the context of a work-from-home environment. Employees' intention to violate an organization's established ISPs while working outside of the traditional office environment could be distinctly different from work-from-office practice. Organizations should be aware of the neutralization techniques, and proactive measures should be taken such that employees comply with ISP. This study will further involve large sample data collection through a survey instrument, and test the hypotheses posited in this model. Findings from this research would guide organizations in implementing effective measures to mitigate the risks introduced by the workplace shift. Along with the technical controls, organizations should also consider the behavioral aspects of employees in mitigating ISP violations and insider threats.

REFERENCES

Barlow, J., Warkentin, M., Ormond, D., & Dennis, A. 2013. Don't make excuses! Discouraging neutralization to reduce IT policy violation. Computers & Security, 39(Part B), 145-159.

Chan, M., Woon, I., & Kankanhalli, A. 2005. Perceptions of information security in the workplace: Linking information security climate to compliant behavior. Journal of Information Privacy and Security, 1(3), 18-41.

Cybersecurity Insiders. 2021 "Insider Threat Report" (https://www.cybersecurity-insiders.com/wp-content/uploads/2021/06/2021-Insider-Threat-Report-Gurucul-Final-dd8f5a75.pdf; accessed June 30, 2023)

D'Arcy, J., & Lowry, P. B. 2019. Cognitive-affective drivers of employees' daily compliance with information security policies 1: A multilevel, longitudinal study. Information Systems Journal, 29(1), 43-69.

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.

Farshadkhah, S., Van Slyke, C., & Fuller, B. 2021. Onlooker effect and affective responses in information security violation mitigation. Computers & Security, 100, 102082.

Guan, B., & Hsu, C. 2020. The role of abusive supervision and organizational commitment on employees' information security policy noncompliance intention. Internet Research, 30(5), 1383-1405.

Gwebu, K. L., Wang, J., & Hu, M. Y. 2020. Information security policy noncompliance: An integrative social influence model. Information Systems Journal, 30(2), 220-269.

IBM Security. 2021. "X-Force Insider Threat Report "(https://www.ibm.com/downloads/cas/BLRZYM03; accessed June 30, 2023)

INSA. 2021. "Managing Insider Threats in a Remote Work Environment: Lessons from the Pandemic"(https://www.insaonline.org/docs/default-source/default-document-library/2022-white-papers/insa-wp-pandemic-v4.pdf; accessed June 30, 2023)

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. 2016. Dispositional and situational factors: Influences on information security policy violations. European Journal of Information Systems, 25(3), 231-251.

Klockars, C. B. 1974. The professional fence. New York: Free Press.

Li, H., Luo, X. R., & Chen, Y. 2021. Understanding information security policy violation from a situational action perspective. Journal of the Association for Information Systems, 22(3), 5.

Li, Y., Pan, T., & Zhang, N. 2020. From hindrance to challenge: How employees understand and respond to information security policies. Journal of Enterprise Information Management, 33(1), 191-213.

Li, Y., Xin, T., & Siponen, M. 2022. Citizens' cybersecurity behavior: Some major challenges. IEEE Security & Privacy, 20(1), 54-61. doi: 10.1109/MSEC.2021.3117371

Lowry, P. B., Moody, G. D., Galletta, D. F., & Vance, A. 2013. The drivers in the use of online whistle-blowing reporting systems. Journal of Management Information Systems, 30(1), 153-190.

Minor, W. W. 1981. Techniques of Neutralization: A Reconceptualization and Empirical Examination. Journal of Research in Crime and Delinquency, 18(2), 295–318.

Nasirpouri Shadbad, F., & Biros, D. 2022. Technostress and its influence on employee information security policy compliance. Information Technology & People, 35(1), 119-141.

Ogbanufe, O., Crossler, R. E., & Biros, D. 2023. The valued coexistence of protection motivation and stewardship in information security behaviors. Computers & Security, 124, 102960.

Ormond, D., Warkentin, M., & Crossler, R. E. 2019. Integrating cognition with an affective lens to better understand information security policy compliance. Journal of the Association for Information Systems, 20(12), 4.

Ponemon. 2022. "Cost of Insider Threats Global Report" (https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats; accessed June 30, 2023)

Silic, M., Barlow, J. B., & Back, A. 2017. A new perspective on neutralization and deterrence: Predicting shadow IT usage. Information & Management, 54(8), 1023-1037.

Siponen, M., & Vance, A. 2010. Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487-502.

Sykes, G., & Matza, D. 1957. Techniques of neutralization: A theory of delinquency. American Sociological Review, 22(6), 664-670.

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

Trinkle, B. S., Warkentin, M., Malimage, K., & Raddatz, N. 2021. High-risk deviant decisions: Does neutralization still play a role? Journal of the Association for Information Systems, 22(3), 3.

Vance, A., Siponen, M. T., & Straub, D. W. 2020. Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. Information & Management, 57(4), 103212.

Willison, R., Warkentin, M., & Johnston, A. C. 2018. Examining employee computer abuse intentions: Insights from justice, deterrence, and neutralization perspectives. Information Systems Journal, 28(2), 266-293.

Yazdanmehr, A., & Wang, J. 2021. Can peers help reduce violations of information security policies? The role of peer monitoring. European Journal of Information Systems.

Yazdanmehr, A., Li, Y., & Wang, J. 2022. Does stress reduce violation intention? Insights from eustress and distress processes on employee reaction to information security policies. European Journal of Information Systems, 1-19.

Yazdanmehr, A., Li, Y., & Wang, J. 2023. Employee responses to information security related stress: Coping and violation intention. Information Systems Journal.

Zhen, J., Xie, Z., Dong, K., & Chen, L. 2022. Impact of negative emotions on violations of information security policy and possible mitigations. Behaviour & Information Technology, 41(11), 2342-2354.