The Spillover Effect of Workplace Cybersecurity Training on Home Cyber Hygiene

Weiyu Wang[1]
Price College of Business School,
University of Oklahoma,
Norman, OK, United States

Matthew Jensen
Price College of Business School,
University of Oklahoma,
Norman, OK, United States

ABSTRACT

This study explores the potential spillover effect of workplace cybersecurity training on home contexts, hypothesizing that such training may enhance home cyber hygiene behaviors, providing additional protection against cyber threats. Using psychological empowerment as a theoretical foundation, we investigate the impact of organizational cybersecurity training on individuals' security practices beyond the workplace.

Keywords: Cybersecurity Training, Digital Hygiene, Remote Work, Psychological Empowerment, Spillover Effect.

INTRODUCTION

Cybersecurity literature has often focused on organizational settings and workplace security measures. These are environments over which organizations have the most control and, until recently, locations in which most value-producing activities take place. Much less academic attention has been focused on cybersecurity measures at home (Li and Siponen 2011). Yet, protection from cyber threats at home is critical for individuals as they go about their lives and pursue their interests. The consequences of insecure personal computing environments can be costly. For example, in 2023, identity theft cost US consumers $43 billion (Sando 2024), and the average cost of a data breach rose to $4.45 million (IBM 2023).

To counter the rising frequency and sophistication of cyber threats, organizations invest heavily in cybersecurity training. By 2027, these investments are projected to exceed $10 billion (Morgan 2023). There may be significant, thus far unrecognized, benefits for individuals

[1] Corresponding author. weiyuwang-1@ou.edu.

participating in these initiatives. Specifically, there could be a spillover effect of workplace cybersecurity training on workers' digital hygiene practices at home. Similar spillover effects between work and home have been observed in job satisfaction, mood, and technostress (Benlian 2020; Judge and Ilies 2004). Therefore, we expect similar effects for participants in workplace cybersecurity training. This research answers the call to understand home users' information security behavior, especially regarding knowledge transfers from organizational to home contexts (Li and Siponen 2011). We aim to address the question: *How does participation in workplace cybersecurity training affect employees' digital hygiene practices at home?*

Adopting a theoretical lens grounded in psychological empowerment, we propose that workplace cybersecurity training influences employees' perceptions of competence, control, meaning, and impact concerning cyber hygiene practices. These perceptions, in turn, can affect employees' engagement in coping strategies when facing cybersecurity threats at home. We will employ a multimethod empirical approach, combining surveys and experiments, to investigate our research question. Multimethod inquiry is proper in complex real-world problem situations (Mingers 2003). The findings are expected to offer valuable insights into the unappreciated benefits of cybersecurity training, potentially enhancing employees' overall digital resilience. It underscores the importance of practical cybersecurity training in promoting comprehensive cybersecurity practices that extend beyond the organizational perimeter.

LITERATRUE REVIEW

Workplace Cybersecurity Training and Cybersecurity Behaviors

Companies that implement and enforce comprehensive cybersecurity awareness training among their employees effectively promote a widespread understanding of cyber threats across the organization (Hart et al. 2020). The knowledge and insights acquired by employees through cybersecurity awareness training can significantly mitigate cybersecurity risks by enabling end-users to take proactive measures (Zwilling et al. 2022). In remote working contexts, cybersecurity awareness is a significant mediating prerequisite to precautionary behaviors (Nwankpa and Datta 2023). However, the impact of cybersecurity training on behavior varies significantly. While security training has been proven effective in discerning cyber-attacks and reducing the number of incidents (Kweon et al. 2021), some suggest its effectiveness may be limited (Aldawood and Skinner 2019). Literature shows that training recency, materials, and methods all affect individuals' information security policy compliance (Vedadi et al. 2024). Furthermore, the context of non-work at home is still overlooked (Li and Siponen 2011). These findings underscore the need for cybersecurity training to educate employees on cyber threats directly related to contextualized information security.

Digital Hygiene Practices and Work-Home Spillover

Cyber hygiene refers to the cyber security practices that individuals should use to protect the safety and integrity of their personal information on Internet-enabled devices from being compromised in a cyberattack (Vishwanath et al. 2020). In IS research, individual-level digital hygiene has been studied in the workplace (Bulgurcu et al. 2010; Siponen and Vance 2010) and home settings (Anderson and Agarwal 2010; Thompson et al. 2017), but no studies focus on the spillover of individual behavior in different contexts.

Spillover refers to the "effects of work and family on one another that generate similarities between the two domains" (Edwards and Rothbard 2000, p. 3). These similarities are evidenced in affect (i.e., mood and satisfaction), values (i.e., the importance ascribed to pursuits), skills, and behaviors. We define work-home spillover as the transfer of skills, behaviors, affect, and values from the workplace to a remote domain (e.g., home) (Sok et al. 2014). Work-home spillover has been used to explain the "process through which work-family are linked" (Lambert 1990, p. 239). Research indicates that employees' emotions, attitudes, skills, and behaviors at work can carry over into their family life (Lambert 1990).

The spillover effect can be direct. For instance, employees using a work-provided VPN for personal activities and browsing at home can protect their online privacy and secure data transmission. Similarly, employees might change the default password on their home routers after cybersecurity training. But the spillover can also be indirect. For instance, workplace cybersecurity training may increase the workers' awareness of cyber issues and the threat to their financial data. Enhanced phishing awareness from workplace training might spill over into personal activities, leading employees to be more cautious about unsolicited emails and links in their private email accounts. Although work-home spillover has been widely studied regarding job satisfaction, mood (Judge and Ilies 2004), and technostress (Benlian 2020), to our knowledge, no cybersecurity research in the IS literature investigated cybersecurity behavior at the work-life boundary.

THEORETICAL FOUNDATION AND HYPOTHESIS DEVELOPMENT

Psychological Empowerment

Empowerment is a multilevel construct that can be either a process or an outcome (Zimmerman 1995). Empowering processes refer to situations where individuals have or are allowed to influence the decisions that affect their lives and control their destinies. Workplace cybersecurity training and participation in information systems decision-making are two examples of empowering processes in cybersecurity (Dhillon et al. 2020).

In IS cybersecurity studies, researchers adopt four cognitive dimensions of psychological empowerment, including competence, autonomy, meaning, and impact (Dhillon et al. 2020;

Spreitzer 1995), to study empowered outcomes. *Competence*, or self-efficacy, refers to the belief in one's "capability to perform activities with skill" (Spreitzer 1995, p. 1443). Workplace cybersecurity training increases employees' awareness, knowledge, and capability to perform tasks skillfully. *Autonomy*, or self-determination, refers to one's sense of having a choice in initiating and regulating actions (Spreitzer 1995). For instance, work structures that allow employees to be involved in decision-making make them feel a greater sense of autonomy (Dhillon et al. 2020). *Impact* refers to the extent to which an individual can affect outcomes, while *meaning* refers to the alignment between a goal's requirements and an individual's ideals, values, beliefs, and behaviors (Spreitzer 1995, Spreitzer et al. 1997). In the workplace, providing awareness training and access to security resources can help employees view a task as manageable and important, enabling them to see how their efforts can contribute to the organization's goals. This study will focus on the four dimensions of psychological empowerment as the mechanism affecting employee cyber hygiene practices. Figure 1 shows our research model.

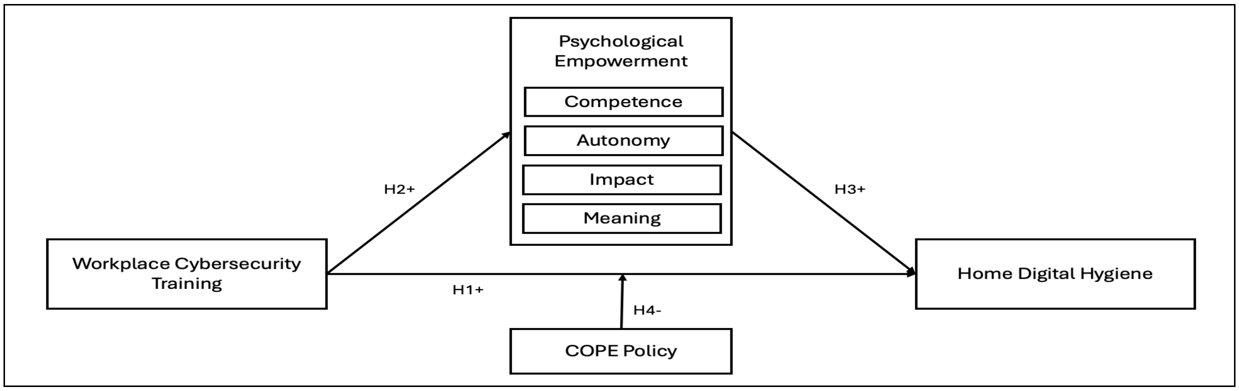

Figure 1. Research Model

Hypothesis Development

Cybersecurity training improves employees' workplace digital hygiene by equipping employees with the necessary skills and knowledge (Alyami et al. 2023; Jensen et al. 2017). We argue that participating in cybersecurity training will also have a direct effect on home hygiene behavior, such that many hygiene behaviors directly transfer and apply in the home environment.

H1: Workplace cybersecurity training is positively associated with home digital hygiene.

Workplace cybersecurity training can increase awareness of cybersecurity risks (D'Arcy et al. 2009), helping people realize how vulnerable their home environment is to cyberattacks. Despite awareness of their role in mitigating cyber threats, individuals often underestimate the importance of cybersecurity practices (Herath and Rao 2009). This undervaluation is partly due to the perceived conflict between cybersecurity requirements and workplace productivity or the willingness to assist coworkers (Posey and Shoss 2022). At home, individuals may mistakenly believe that hackers primarily target large organizations or high-profile figures, leading to the misconception that maintaining cyber hygiene is not a priority. However, workplace cybersecurity training, particularly those emphasizing the direct impact on individuals, can help reinforce the belief that cyber hygiene practices align with their goal of keeping productivity and personal data safe. Autonomy is generally greater at home than in the workplace, as individuals have more freedom to make decisions. Cybersecurity training enhances this sense of autonomy by providing strategies to defend against cyber threats. Competence, including knowledge and skills from workplace training, can transfer to the home context. We hypothesize that,

H2: Workplace cybersecurity training is positively associated with employees' psychological empowerment in the home context.

Empowerment will make employees more inclined to adopt positive attitudes toward cyber hygiene practices (Dhillon et al. 2020). Employees who feel competent and autonomous are more likely to apply workplace cybersecurity training at home. For example, individuals who believe they have the skills to secure their devices are more likely to create strong passwords or enable multi-factor authentication at home. As a result, they are more likely to use task-focused coping mechanisms instead of emotion-focused or avoidance coping strategies. These adaptive coping responses will increase their efforts in implementing home digital hygiene practices.

H3: Employee's psychological empowerment is positively associated with home digital hygiene.

The delineation between work and home environments can significantly influence the spillover of behaviors and attitudes from one domain to another (Benlian 2020). In cybersecurity, the Corporate-Owned, Personally Enabled (COPE) strategy might moderate the link between digital hygiene practices at work and home. Employees using COPE devices may assume that their organization has already implemented robust cybersecurity measures, thus believing that their data is automatically protected. This assumption can reduce proactive cybersecurity behaviors in their home settings (Nwankpa and Datta 2023). Organizational controls in COPE devices may inadvertently decrease individual vigilance and responsibility toward personal cybersecurity at home, potentially weakening the sense of competence and control.

H4: A COPE policy negatively moderates the relationship between workplace cybersecurity training and home digital hygiene behaviors.

RESEARCH METHOD

This work will adopt a multi-method approach to study the potential effects of spillover. In Study 1, a survey and semi-structured interviews will be used to collect data from a sample of employees who have just been recruited by an organization that will have cybersecurity training at their workplace. We will ask about their home digital hygiene behavior (before cybersecurity training). After completing the training, they will be asked to complete a survey questionnaire that includes items that measure the extent to which respondents apply cybersecurity principles to their digital hygiene when home and their perceptions of the benefits and drawbacks of workplace training on personal cybersecurity. The semi-structured interviews will provide indepth insights into the participants' experiences and perspectives regarding workplace and home digital hygiene practices.

In study 2, we will conduct a 2 (with vs. without cybersecurity training) * 2 (enabling vs. not enabling COPE) between-subject, scenario-based experiment. We will ask participants to envision themselves as new employees. They will be required to create a mock workplace account and a cloud services account that can be used for work and personal purposes. The participants will be randomly assigned to one of the four groups. All participants will be allowed to change those passwords after the experiment. They will be asked to complete the questionnaire about psychological empowerment and coping adaptiveness at the end of the experiment (see appendix).

EXPECTED CONTRIBUTION, LIMITATION, AND FUTURE WORK.

The shift to hybrid workplaces has heightened the challenge of securing organizational data. This study examines how workplace training influences home cybersecurity hygiene behaviors, revealing the previously hidden impacts of workplace cybersecurity training. By integrating contextual factors such as COPE policies, this study provides a nuanced understanding of how empowerment influences cybersecurity practices across different settings. This study also offers actionable insights for organizations to structure device usage policies. However, the study has limitations, including potential biases from self-reported data. The moderators may not capture the full range of contextual nuances. Future research could address these limitations by employing longitudinal designs to capture behavioral changes over time and exploring additional factors, such as home dynamics or shared device usage, that may moderate the relationship between workplace cybersecurity training and home digital hygiene.

REFERENCES

Alyami, A., Sammon, D., Neville, K., and Mahony, C. 2023. "The Critical Success Factors for Security Education, Training and Awareness (Seta) Program Effectiveness: A Lifecycle Model," *Information Technology & People* (36:8), pp. 94-125.

Anderson, C. L., and Agarwal, R. 2010. "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS quarterly*), pp. 613-643.

Benlian, A. 2020. "A Daily Field Investigation of Technology-Driven Spillovers from Work to Home," *MIS quarterly* (44:3).

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

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.

Dhillon, G., Abdul Talib, Y. Y., and Picoto, W. N. 2020. "The Mediating Role of Psychological Empowerment in Information Security Compliance Intentions," *Journal of the Association for Information Systems* (21:1), p. 5.

Edwards, J. R., and Rothbard, N. P. 2000. "Mechanisms Linking Work and Family: Clarifying the Relationship between Work and Family Constructs," *Academy of management review* (25:1), pp. 178-199.

Hart, S., Margheri, A., Paci, F., and Sassone, V. 2020. "Riskio: A Serious Game for Cyber Security Awareness and Education," *Computers & Security* (95), p. 101827.

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.

IBM. 2023. "Cost of a Data Breach Report 2023."

Jensen, M. L., Dinger, M., Wright, R. T., and Thatcher, J. B. 2017. "Training to Mitigate Phishing Attacks Using Mindfulness Techniques," *Journal of Management Information Systems* (34:2), pp. 597-626.

Judge, T. A., and Ilies, R. 2004. "Affect and Job Satisfaction: A Study of Their Relationship at Work and at Home," *Journal of applied psychology* (89:4), p. 661.

Lambert, S. J. 1990. "Processes Linking Work and Family: A Critical Review and Research Agenda.," *Human relations,* (43:3), pp. 239-257.

Li, Y., and Siponen, M. 2011. "A Call for Research on Home Users' Information Security Behaviour,").

Mingers, J. 2003. "The Paucity of Multimethod Research: A Review of the Information Systems Literature," *Information systems journal* (13:3), pp. 233-249.

Morgan, S. 2023. "Security Awareness Training Market to Hit $10 Billion Annually by 2027," in: *CyberCrime Magazine*.

Nwankpa, J. K., and Datta, P. M. 2023. "Remote Vigilance: The Roles of Cyber Awareness and Cybersecurity Policies among Remote Workers," *Computers & Security* (130), p. 103266.

Posey, C., and Shoss, M. 2022. "Research: Why Employees Violate Cybersecurity Policies," *Harvard Business Review*).

Sando, S. 2024. "2024 Identity Fraud Study: Resolving the Shattered Identity Crisis." from https://www.javelinstrategy.com/research/2024-identity-fraud-study-resolving-shattered-identity-crisis

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS quarterly*), pp. 487-502.

Sok, J., Blomme, R., and Tromp, D. 2014. "Positive and Negative Spillover from Work to Home: The Role of Organizational Culture and Supportive Arrangements," *British Journal of Management* (25:3), pp. 456-472.

Spreitzer, G. M. 1995. "Psychological Empowerment in the Workplace: Dimensions, Measurement, and Validation," *Academy of management Journal* (38:5), pp. 1442-1465.

Thompson, N., McGill, T. J., and Wang, X. 2017. "“Security Begins at Home”: Determinants of Home Computer and Mobile Device Security Behavior," *computers & security* (70), pp. 376-391.

Vedadi, A., Warkentin, M., Straub, D. W., and Shropshire, J. 2024. "Fostering Information Security Compliance as Organizational Citizenship Behavior," *Information & Management* (61:5), p. 103968.

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., and Chin, J. 2020. "Cyber Hygiene: The Concept, Its Measure, and Its Initial Tests," *Decision Support Systems* (128), p. 113160.

Zimmerman, M. A. 1995. "Psychological Empowerment: Issues and Illustrations," *American journal of community psychology* (23), pp. 581-599.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., and Basim, H. N. 2022. "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study," *Journal of Computer Information Systems* (62:1), pp. 82-97.

APPENDIX A – MEASUREMENT

Construct	Measurement Items	Reference
Home Psychological Empowerment		
Competence	COMP1: I am confident about my ability to do secure information and information systems at home. COMP2: I am self-assumed about my capabilities to perform securing information and information systems activities. COMP3: I have mastered the skills necessary for securing information and information systems.	(Dhillon et al. 2020; Spreitzer 1995)
Autonomy	AUTO1: I have significant autonomy in determining how I secure information and information systems. AUTO2:I can decide on my own how to secure information and information systems. AUTO2:I have considerable opportunity for independence and freedom in how to secure information and information systems.	(Dhillon et al. 2020; Spreitzer 1995)
Impact	PACT1: My impact of what happens in my home related to information security is large. PACT2: I have a great deal of control over what happens in my home related to information security. PACT3: I have significant influence over what happens in my home related to information security.	(Dhillon et al. 2020; Spreitzer 1995)
Meaning	MEAN1: Securing information and information systems at home is very important to me. MEAN2: Securing information and information systems at home is personally meaningful to me. MEAN3: Securing information and information systems at home is meaningful to me.	(Dhillon et al. 2020; Spreitzer 1995)
Home Digital Hygiene	HDH1: Enabling firewalls on your computing devices at home. HDH2: Running a virus scan on any new external storage device at home. HDH3: Changing default username and password to something unique on all Internet enabled devices at home. HDH4: Managing how your browser stores passwords at home. HDH5: Creating new/unique logins and passwords for all your online sign-ins at home. HDH6: Checking an incoming email's header when checking email at home. HDH7: Checking a sender's email domain name when checking email at home. HDH8: Checking to see if email requests have grammatical or typographical errors when checking email at home	(Vishwanath et al. 2020)