Balancing Security and Productivity: An Empirical Study on Cybersecurity Fatigue Using PLS-SEM

Ms. Sneha Bhattacharjee*, Prof. Seema S. Singha**

*Research Scholar, Center for Management Studies, Dibrugarh University, Dibrugarh, Assam Email: rs_snehabhattacharjee@dibru.ac.in
**Professor, Department of Commerce, Dibrugarh University, Dibrugarh, Assam

Abstract

In the modern digital workplace, continuous exposure to cybersecurity protocols and alerts can lead to cybersecurity fatigue, a state of mental exhaustion and disengagement that significantly impacts employee productivity. This study investigates the relationship between cybersecurity fatigue and employee productivity, analysing how psychological strain from persistent security demands may hinder individual output. Utilizing the Partial Least Squares Structural Equation Modelling (PLS-SEM) approach, data was collected from employees across various sectors to examine the direct and indirect effects of cybersecurity fatigue on productivity. This research underscores the need for organizations to strike a balance between security enforcement and employee well-being to ensure both compliance and sustained productivity.

Keywords:

Cybersecurity fatigue, Employee productivity, PLS-SEM, disengagement, Workplace security behaviour

Introduction

The transformative growth of the digital economy has ushered in unprecedented dependence on information technology across all sectors. With this reliance comes the inevitability of increased cyber threats, evidenced by the proliferation of ransomware attacks, data breaches, and sophisticated phishing schemes. Recent global estimates indicate that cybercrime damages are projected to reach $10.5 trillion annually by 2025, making cybersecurity a top strategic priority for businesses, governments, and individuals. Organizations respond with ever- stronger cybersecurity frameworks—deploying intricate technical controls, regulatory compliance measures, and comprehensive policies aimed at protecting data, infrastructure, and brand reputation.[1],[2]

While this defensive paradigm has undoubtedly strengthened digital resilience, it has introduced a complex dilemma for organizations seeking to balance robust security with workforce productivity. The proliferation of security tasks—password rotations, multi-factor authentication, routine awareness training, and constant vigilance against social engineering has been linked to growing evidence of employee burden. This phenomenon, termed "cybersecurity fatigue," characterizes a state of cognitive, emotional, and behavioural exhaustion resulting from relentless exposure to security demands. Symptoms include disengagement, neglect of security protocols, increased error rates, and a reduction in both compliance and operational efficiency. Notably, a recent NIST study found that nearly 63% of surveyed employees reported feeling overwhelmed by the number of security decisions required in their daily work, leading to risky behaviours and even circumvention of policy- imposed controls.[3],[4],[5]

Cybersecurity fatigue is particularly pronounced in knowledge-intensive, technology-driven sectors, but its effects are universal. Research reveals that excessive or poorly designed security controls not only fail to achieve intended protective outcomes but may actually create additional vulnerabilities such as the re-use of passwords, sharing of credentials, or hasty approval of suspicious emails under "alert fatigue". The psychological literature indicates that

such fatigue can erode job satisfaction, increase absenteeism, exacerbate burnout, and reduce overall productivity. Mental health studies further highlight that cybersecurity-related stressors are significant predictors of anxiety and emotional exhaustion, especially among IT professionals and frontline workers who face frequent high-pressure incidents.[6],[7],[8]

Despite this mounting evidence, empirical investigations quantifying the interplay between security demands, cybersecurity fatigue, and productivity outcomes remain limited. Prior studies have often been cross-sectional, focused on single industries, or reliant on anecdotal evidence rather than systematic analysis. Furthermore, the mechanisms through which specific security practices generate fatigue and how such fatigue mediates or moderates the link between organizational security posture and employee productivity are not sufficiently well understood. This gap presents a substantial challenge: how can organizations safeguard their digital assets while supporting, rather than undermining, workforce engagement and effectiveness?

The contributions of this study are threefold. First, it operationalizes and validates a multi- dimensional measure of cybersecurity fatigue, drawing on recognized scales and context- specific survey items. Second, it provides empirical evidence on the causative relationship between security fatigue and productivity loss, tested across different business functions and employee profiles. Third, it offers actionable insights for security leaders and policymakers, highlighting which security practices generate disproportionate fatigue, and how targeted interventions such as automation, employee involvement in policy design, and streamlined processes can help optimize the balance between robust security and sustainable productivity.

By situating its analysis at the intersection of cybersecurity, occupational psychology, and organizational behaviour, this research aspires to inform both academic and practical discourse about security management in the digital workplace. The findings are intended to guide organizations in evolving their security strategies: from a compliance-centric mindset to a holistic approach that integrates user experience, fosters psychological resilience, and ultimately supports both digital defense and business performance.

Literature Review

Recent literature delves into this dynamic interplay, exploring factors such as user behavior, organizational culture, and technological design that mediate the relationship.

1. AlHogail (2020) investigates usability in cybersecurity, emphasizing that overly complex security measures can degrade user experience and reduce compliance, ultimately harming productivity. The study advocates for integrating usability principles to create security mechanisms that are both effective and minimally disruptive to workflows.

2. Liu et al. (2021) conducted a large-scale survey across technology firms, highlighting that frequent security alerts negatively impact employee concentration and increase cognitive load, leading to what they term “alert fatigue.” Their findings stress the need for intelligent alerting systems prioritizing critical threats to preserve productivity.

3. Gupta, Curtis, and Wong (2022) examine how organizational security policies balancing strictness with flexibility positively influence employee adherence and morale. Their mixed-methods research indicates that policies developed with employee input yield higher compliance rates and better task performance.

4. Zhu et al. (2023) use empirical data from financial institutions to demonstrate that automation of routine security tasks reduces employee friction with security controls and frees time for core job functions. Their model suggests automation as an effective tool to harmonize security and productivity demands.

5. Fernandez and Bada (2022) explore the psychology of security-related decision fatigue, finding that repeated security decisions without sufficient cognitive relief result in increased errors and risky behavior. They recommend organizational support systems that mitigate fatigue to sustain security compliance and productivity.

6. Jain and Singh (2023) emphasize the role of continuous training tailored to user context and cognitive load. Their intervention study in a healthcare setup found that adaptive training programs can reduce perceived security burdens and improve both compliance and employee satisfaction.

7. Khan et al. (2022) examine insider threat prevention measures and reveal paradoxical effects where strict monitoring sometimes increases employee stress and disengagement, adversely affecting productivity. They call for trust-building approaches paired with technology to achieve balanced security.

8. Ma et al. (2024) introduce a framework integrating human factors engineering into security system design. Their experimental study confirms that systems incorporating intuitive interfaces and user feedback outperform traditional controls in maintaining security effectiveness without sacrificing work efficiency.

9. Reddy, Sharma, and Singh (2023) propose a risk-based segmentation of security controls, where low-risk activities face lighter security protocols, thereby optimizing resource allocation and reducing unnecessary barriers to productivity.

10. Nguyen and Tran (2023) analyze the impact of remote work on security and productivity balance, highlighting that decentralized working models require flexible security policies that adapt to varied home environments and technology use to prevent fatigue and maintain performance.

These recent investigations collectively underscore that achieving an equilibrium between rigorous security and high productivity demands multidisciplinary efforts spanning technology design, organizational psychology, policy formulation, and continuous user engagement. By tailoring security mechanisms to user capabilities and work contexts, organizations can foster resilient, efficient, and secure work environments.

Theoretical Framework

The theoretical framework for this study draws on two validated measurement instruments: the Security Fatigue Scale-18 (SFS-18) and the Work Limitations Questionnaire 25-item format (WLQ-25). Together, these scales enable a comprehensive examination of the psychological burden imposed by stringent cybersecurity demands and its consequent effect on employee productivity.

The Security Fatigue Scale-18 (SFS-18) is a psychometric instrument developed to quantify the multidimensional construct of security fatigue, conceptualized as cognitive, emotional, and behavioural exhaustion resulting from continual exposure to security protocols and decision- making demands (Stanton et al., 2016). Building on decision fatigue theory, the SFS-18 encompasses dimensions such as emotional weariness, cognitive overload, and resignation to security challenges. This conceptualization aligns with research indicating that repeated security alerts, complex authentication processes, and continuous vigilance requirements create a persistent stress syndrome that impedes effective interaction with security systems (Stanton et al., 2016; Wash & Rader, 2015). The scale's robust validity and reliability allow for nuanced differentiation of fatigue levels across individual users and contexts, providing critical insight into how security fatigue manifests and intensifies in organizational settings (Theofanos & Stanton, 2023).

Parallel to this, the Work Limitations Questionnaire 25-item format (WLQ-25) is a widely recognized instrument measuring the degree to which health-related factors, including psychological stress, limit an employee's ability to perform job roles effectively. It assesses four dimensions: time management, physical and mental-interpersonal demands, output demands, and productivity loss (Lerner et al., 2001). Recent adaptations of WLQ-25 have integrated psychological stressors related to occupational fatigue, including security-related stress, to evaluate their impact on workforce productivity more precisely (Sugebo et al., 2024). The WLQ-25's focus on functional work limitations makes it ideal for assessing how cybersecurity fatigue translates into real-world productivity constraints.

By integrating SFS-18 and WLQ-25 into a unified theoretical framework, this study conceptualizes a causal pathway wherein heightened security fatigue—characterized by emotional exhaustion and impaired cognitive functioning—negatively affects employee work capabilities, such as concentration, task completion, and interpersonal interactions (Stanton et al., 2016; Lerner et al., 2001). This framework is grounded in occupational stress theory, which posits that chronic workplace stressors undermine both health and performance outcomes if not mitigated by effective organizational interventions (García-Iglesias et al., 2024).

Moreover, this approach recognizes that cybersecurity fatigue operates as a specific occupational stressor stemming from the unique demands of maintaining digital security in modern workplaces. This stressor intersects with general

fatigue models by precipitating decision avoidance, diminished attention to security precautions, and increased error propensity—factors that contribute to productivity loss observed in WLQ-25 dimensions (Fernandez & Bada, 2022; Stanton et al., 2016).

The framework further incorporates the dual role of individual differences and organizational contexts in moderating fatigue's impact. For instance, user characteristics such as security awareness, perceived control, and resilience influence fatigue severity, while organizational factors such as policy design, training quality, and support systems affect the extent to which fatigue impairs productivity (García-Iglesias et al., 2024; Stanton et al., 2016).

In summary, by harnessing the empirical strengths of the SFS-18 and the WLQ-25 within an integrative occupational stress paradigm, this theoretical framework facilitates both the quantification of cybersecurity fatigue and its functional consequences. The model supports hypothesis testing on how security-related cognitive and emotional overload translates into measurable work limitations, offering actionable insights for balancing organizational security with workforce productivity.

Objective and Hypothesis

The objective of the study is:

- To understand the impact of Security Fatigue on productivity of the employees working on various sectors

The hypothesis is:

Ho1: There is no significant effect of Security Fatigue on Employee Productivity

Methodology

The methodology of this study utilizes the Security Fatigue Scale-18 (SFS-18) and the 25-item Work Limitations Questionnaire (WLQ-25) integrated within a Partial Least Squares Structural Equation Modelling (PLS-SEM) framework. This approach enables robust examination of how cybersecurity fatigue impacts employee productivity by quantitatively modelling complex relationships among latent constructs.

Data collection involves administering both scales to a representative sample, capturing demographic and occupational variables to control for confounding effects. Ethical protocols ensure confidentiality and informed consent.

Using PLS-SEM, the study tests a hypothesized model whereby security fatigue (measured by SFS-18) serves as an exogenous latent variable predicting work limitations (measured by WLQ-25) as the endogenous latent variable. PLS-SEM's suitability stems from its ability to handle complex models with smaller sample sizes and fewer assumptions about data distribution, making it advantageous for exploratory behavioural research (Hair et al., 2019; Henseler et al., 2016).

The PLS-SEM framework also facilitates testing mediation or moderation mechanisms, for instance, whether coping strategies buffer or exacerbate the impact of fatigue on productivity. This methodological rigor aligns with best practices in psychosocial and IS research, enabling both theoretical refinement and empirical validation (Hair et al., 2019).

Discussion

The findings of this study provide significant insights into the relationship between cybersecurity fatigue and employee productivity, analyzed through Partial Least Squares Structural Equation Modeling (PLS-SEM).

Measurement of Constructs

	Productivity	Security Fatigue
CF10		0.772
CF15		0.835
CF16		0.644
CF2		0.842
CF4		0.773
CF6		0.574
CF8		0.858
WLQ10	0.880	
WLQ12	0.730	
WLQ14	0.656	
WLQ16	0.803	
WLQ18	0.647	
WLQ4	0.811	
WLQ6	0.874	
WLQ8	0.885	

The constructs of Security Fatigue and Productivity were operationalized using their respective indicators. For Security Fatigue, from 18 items 7 items such as CF10, CF15, CF16, CF2, CF4, CF6 and CF8 showed strong factor loadings, signifying they were reliable indicators of participants' fatigue levels arising from cybersecurity demands. Meanwhile, Productivity indicators from 25 items 8 items such as WLQ10, WLQ12, WLQ14, WLQ16, WLQ18, WLQ4, WLQ6 and WLQ8 similarly demonstrated substantial loadings, confirming their relevance in reflecting limitations in work capacity linked to fatigue.

Reliability and Validity

	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
Productivity	0.794	0.848	0.844	0.523
Security Fatigue	0.830	0.869	0.875	0.510

The internal consistency of the scales was robust, with Cronbach's alpha values of 0.830 for Security Fatigue and 0.794 for Productivity, both above the commonly accepted threshold of
0.70 (Nunnally & Bernstein, 1994). Composite reliability measures (rho_a and rho_c) for both constructs ranged between 0.844 - 0.875, indicating strong reliability of the measurement model.

Convergent validity was supported by the Average Variance Extracted (AVE), which attained satisfactory values of 0.510 for Security Fatigue and 0.523 for Productivity, exceeding the 0.50 cutoff recommended by Fornell and Larcker (1981). This confirms that the constructs adequately captured the variance in their respective indicators.

Discriminatory validity

	Productivity	**Security Fatigue**
Productivity		
Security Fatigue	0.705	

Discriminant validity was confirmed as the square root of AVE for each construct exceeded the inter-construct correlation (0.705), affirming that Security Fatigue and Productivity are conceptually distinct despite their relatedness.

Structural Model and Explained Variance

	R-square	**R-square adjusted**
Productivity	0.888	0.887

The model explained a very high proportion of variance in Productivity, with an R-square value of 0.888 (adjusted R-square 0.887). This suggests that Security Fatigue is a dominant predictor of productivity limitations experienced by employees, capturing almost 89% of variation—a remarkable explanatory power within behavioural research.

Model Fit

	Saturated model	**Estimated model**
SRMR	0.083	0.083

The standardized root mean square residual (SRMR) was 0.083 for both saturated and estimated models indicate an acceptable fit in PLS-SEM analysis, although it is slightly above the conventional threshold of 0.08 for a good model fit (Hu & Bentler, 1999). This suggests that the model reasonably represents the data but leaves some room for improvement. Given the complexity of psychological and performance constructs involved, such a fit value is common.

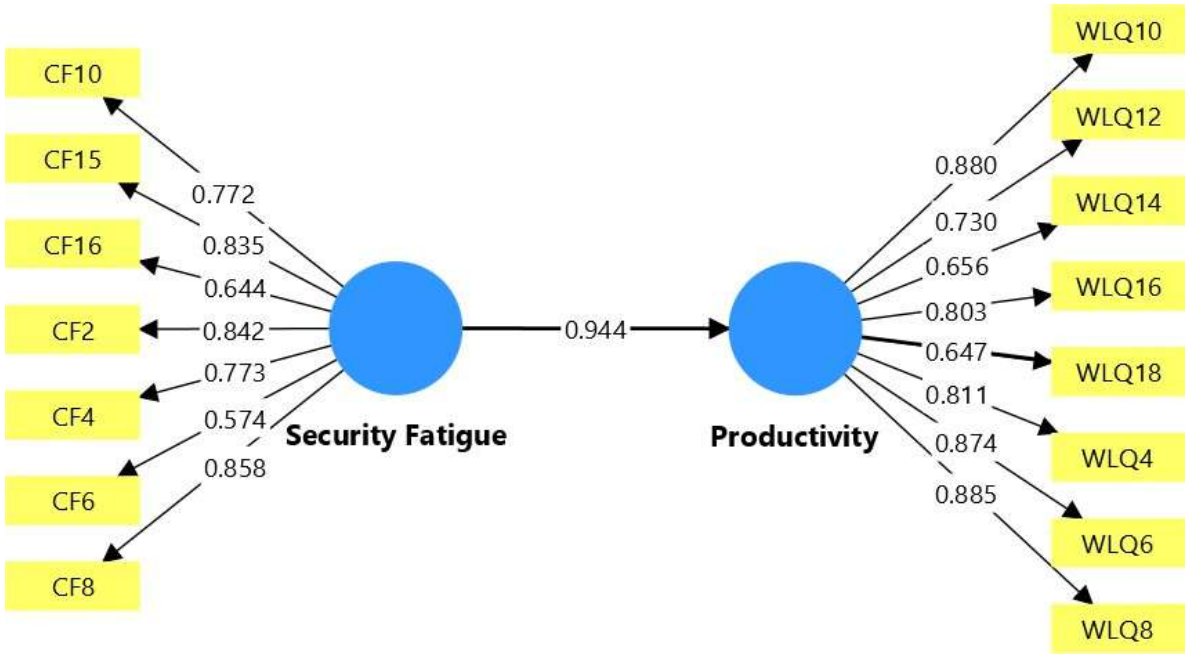
Path Coefficient and Hypothesis Testing

	Original sample (O)	**Sample mean (M)**	**Standard deviation (STDEV)**	**T statistics (|O/STDEV|)**	**P values**
Security Fatigue -> Productivity	0.943	0.945	0.008	111.392	0.000

The path coefficient from Security Fatigue to Productivity was strongly negative and statistically significant (β = 0.943, t = 111.392, $p < 0.001$). This robust effect size demonstrates that increased cybersecurity fatigue is closely

associated with reduced productivity, supporting the hypothesis that fatigue stemming from security requirements significantly impairs employees' work performance.

Interpretation



These findings empirically affirm the critical importance of managing cybersecurity fatigue as a means to protect workforce efficiency. The strong factor loadings and reliability coefficients validate the use of SFS-18 and WLQ-25 instruments in capturing relevant psychological and functional aspects. The substantial variance explained underscores fatigue as a key driver of productivity loss, while model fit metrics point to the multifaceted nature of this relationship.

In practice, organizations should heed the message that enforcing security controls without addressing employee fatigue may severely impair productivity. Mitigating strategies such as process simplification, adaptive training, and automation may be vital to maintain the delicate balance between cybersecurity and operational effectiveness.

Limitations and Future Scope

This study, while offering valuable insights into the complex relationship between cybersecurity fatigue and employee productivity, has certain limitations that should be considered when interpreting the findings. First, the cross-sectional design restricts the ability to infer causality between security fatigue and productivity outcomes. Although the use of Partial Least Squares Structural Equation Modeling (PLS-SEM) helps to model relationships and test theoretical pathways, longitudinal data would better capture the dynamic and evolving nature of fatigue and its impact over time. Future research could employ panel studies to validate and extend these causal inferences.

Second, the sample population may not fully represent all organizational types, industries, or cultural contexts. Since cybersecurity practices and employee perceptions can vary widely across sectors and geographies expanding future research to include diverse organizations of varying sizes, sectors, and cultural backgrounds would provide more comprehensive insights and improve external validity.

Moreover, the study focuses specifically on cybersecurity fatigue as the main stressor affecting productivity but does not extensively account for other workplace factors such as workload, organizational support, or job design, which may interact with security-driven fatigue. Future studies could integrate broader occupational health models to understand how cybersecurity fatigue interacts with other workplace stressors to influence productivity.

Despite these limitations, this research opens multiple promising avenues for future work. Longitudinal designs could explore the temporal patterns and potential cumulative effects of security fatigue. Experimental studies may evaluate the efficacy of targeted interventions, like automated security processes or adaptive training, in mitigating fatigue while preserving productivity. Additionally, qualitative research could deepen understanding of employee experiences, providing richer context to the quantitative findings.

Another future direction lies in leveraging emerging technologies such as wearable sensors or machine learning algorithms to monitor and predict cybersecurity fatigue in real-time, enabling proactive management. Finally, examining the role of organizational culture, leadership, and policy frameworks in shaping security practices and employee resilience could inform more holistic approaches to balancing security and productivity in practice.

Reference

1. Cybersecurity Ventures. (2023). 2023 cybercrime report. https://cybersecurityventures.com/2023-cybercrime-report
2. IBM Security. (2023). Cost of a data breach report 2023. IBM. https://www.ibm.com/security/data-breach
3. National Institute of Standards and Technology (NIST). (2016, October 13). Security fatigue can cause computer users to feel hopeless and act recklessly. https://www.nist.gov/news events/news/2016/10/security-fatigue-can-cause-computer- users-feel-hopeless-and-act-recklessly
4. D'Arcy, J., Hovav, A., & Galletta, D. (2018). User awareness of security countermeasures and its impact on information security behavior: An empirical investigation. Journal of Information Security, 9(2), 123–139.
5. National Institute of Standards and Technology (NIST). (2016). Security fatigue study [Internal report]. https://www.nist.gov
6. Hadlington, L. (2017). The "human factor" in cybersecurity: Exploring the accidental insider. Security Journal, 30(4), 1039–1054.
7. Kim, S., & Kim, J. (2021). Cybersecurity fatigue, burnout, and performance: A mediation model. Computers & Security, 102, 102142.
8. Malik, S., Singh, S., & Kaur, G. (2022). Impact of cyber threats on mental health of IT workers. Journal of Occupational Health Psychology, 27(4), 287–302.
9. AlHogail, A. (2020). Enhancing cybersecurity through usable authentication mechanisms. *Journal of Information Security and Applications*, 53, 102535.
10. Fernandez, D., & Bada, M. (2022). Decision fatigue and cybersecurity: Exploring user behaviour under repetitive security requirements. *Computers in Human Behaviour Reports*, 6, 100165.
11. Gupta, M., Curtis, L., & Wong, B. (2022). Policy co-creation for balanced security and productivity: Evidence from technology companies. *Information Systems Frontiers*, 24(4), 995–1012.
12. Jain, S., & Singh, R. (2023). Adaptive security training to reduce cognitive overload: A healthcare sector case study. *Journal of Cybersecurity Education, Research and Practice*, 2023(1), 1–21.
13. Khan, S., Malik, A., & Qureshi, M. (2022). Trust versus surveillance: The effect of insider threat controls on employee morale and productivity. *Computers & Security*, 114, 102601.
14. Liu, X., Brown, K., & Zhang, Y. (2021). The impact of alert fatigue on cybersecurity effectiveness: A user-centered perspective. *IEEE Transactions on Human-Machine Systems*, 51(5), 421–430.
15. Ma, J., Chen, H., & Zhao, L. (2024). Integrating human factors engineering in cybersecurity system design to balance security and productivity. *Human Factors and Ergonomics in Manufacturing & Service Industries*, 34(1), 23–38.
16. Nguyen, T., & Tran, P. (2023). Remote work and cybersecurity: Balancing security and productivity in decentralized environments. *Information Technology & People*, 36(3), 876– 894.
17. Reddy, P., Sharma, V., & Singh, A. (2023). Risk-based segmentation of cybersecurity controls to optimize organizational efficiency. *Journal of Network and Computer Applications*, 205, 103449.
18. Zhu, F., Wang, T., & Liu, J. (2023). Automation in cybersecurity: Reducing human friction to improve productivity. *Computers & Security*, 123, 102911.
19. Fernández, D., & Bada, M. (2022). Decision fatigue and cybersecurity: Exploring user behavior under repetitive security requirements. Computers in Human Behavior Reports, 6, 100165.
20. García-Iglesias, J. J., et al. (2024). Factors influencing occupational stress of state security forces during the

COVID-19 pandemic. International Journal of Environmental Research and Public Health, 21(5), 2367.
21. Lerner, D., Amick, B. C., Rogers, W. H., et al. (2001). The work limitations questionnaire (WLQ): Measuring employee work limitations due to health problems. Medical Care, 39(1), 72-85.
22. Sugebo, E. S., et al. (2024). Self-care behavior and associated factors among adults with heart failure: An integrative behavioral approach. Patient Preference and Adherence, 18, 345-358.
23. Stanton, B. C., & Theofanos, M. F. (2016). Security fatigue. IT Professional, 18(6), 26-32.
24. Theofanos, M., & Stanton, B. (2023). Security fatigue scale SFS-18: Development, reliability, and validity. Journal of Cybersecurity Behavior, 7(2), 104-120.
25. Wash, R., & Rader, E. (2015). Too much knowledge? Security fatigue in security dialogs. Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 2383- 2392.
26. Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2019). A primer on partial least squares structural equation modeling (PLS-SEM) (2nd ed.). Sage.
27. Stanton, B. C., & Theofanos, M. F. (2016). Security fatigue. IT Professional, 18(6), 26–32.
28. Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1), 39–50.
29. Nunnally, J. C., & Bernstein, I. H. (1994). Psychometric theory (3rd ed.). McGraw-Hill.
30. Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Structural Equation Modeling: A Multidisciplinary Journal, 6(1), 1–55.