

Association for Information Systems

## AIS Electronic Library (AISeL)

---

SAIS 2023 Proceedings

Southern (SAIS)

---

7-1-2023

### Security Burnout and Security Policy Compliance Intention

Sumin Kim

Follow this and additional works at: <https://aisel.aisnet.org/sais2023>

---

#### Recommended Citation

Kim, Sumin, "Security Burnout and Security Policy Compliance Intention" (2023). *SAIS 2023 Proceedings*. 36.

<https://aisel.aisnet.org/sais2023/36>

This material is brought to you by the Southern (SAIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in SAIS 2023 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact [elibrary@aisnet.org](mailto:elibrary@aisnet.org).

# SECURITY BURNOUT AND SECURITY POLICY COMPLIANCE INTENTION

**Sumin Kim**

Mississippi State University  
sk2013@msstate.edu

**Kent Marett**

Mississippi State University  
kmarett@msstate.edu

**Mel Fugate**

Mississippi State University  
mfugate@msstate.edu

## ABSTRACT

This paper aims to explore the role of security burnout and its relationship with employees' security behavior. Although information security researchers put their effort to improve employees' security behavior, there is a lack of research considering the consequences of excessive security measures which may lead to security burnout and increase the risk of security negligence. By focusing on security burnout, this study identifies the antecedents of security burnout by using job demands-resources (JD-R) model, which is used to understand job burnout in Management. Therefore, this study potentially makes a valuable contribution to the field of security research by considering security fatigue, its causes, and its negative consequence and finding ways to mitigate them.

## Keywords

Security burnout, job demands-resources model, security policy compliance

## EXTENDED ABSTRACT

Despite continual investment by companies into security training and infrastructure, an organization's own employees continue to be the weakest link in protecting information security, raising the question of whether more security measures are needed to address this problem. While information security is important for protecting an organization's assets, having an excessive number of security measures may lead to "security burnout" or "security fatigue" among employees, which can potentially increase the risk of security negligence. *Security burnout* refers to a state of weariness or reluctance to engage with information security (Stanton et al., 2016). Individuals who have been exposed to a particular control or measure repeatedly may become fatigued by security (Furnell & Thomson, 2009). Security fatigue among employees can significantly undermine an organization's efforts to achieve security and may be brought about by increasing the number of security measures, providing unclear and complicated security-related messages and education, and ignoring employee feedback and participation in the development and implementation of security policies.

Previous research has explored IT-related burnout, its antecedents, and potential consequences, primarily borrowing from the job burnout concept from the Organizational Behavior discipline (Chen, et al., 2020; Choi et al., 2018). Because of its importance of predicting job performance such as job withdrawal, productivity, or effectiveness, job burnout has been an actively researched topic in management. Management scholars have found explanatory value in the job demands-resources (JD-R) model (Demerouti et al., 2001). In turn, this research-in-progress uses the JD-R model and antecedents from qualitative research on security burnout (Cram et al., 2021) to better understand how to improve employees' security compliance related behavior. To measure demand, we adapt scales such as *work impediment*, *appropriateness*, *understandability*, etc. To measure resource, we adapt scales such as *security education and training awareness*, *participation in security decision making*, etc.

Previous studies have mainly focused on ways to improve employees' security behavior without considering potential negative effects of excessive measures. By focusing on the consequences of excessive security measures which cause security fatigue to employees and examining ways to improve their security-related behavior, this study aims to make a valuable contribution to the field of security research. Further study will empirically explore security burnout and its negative consequences such as deviant security behavior.

**REFERENCES**

1. Chen, H., Li, Y., Chen, L., & Yin, J. (2020). Understanding employees' adoption of the Bring-Your-Own-Device (BYOD): the roles of information security-related conflict and fatigue. *Journal of Enterprise Information Management*, 34(3), 770-792.
2. Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81, 42-51.
3. Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2021). When enough is enough: Investigating the antecedents and consequences of information security fatigue. *Information Systems Journal*, 31(4), 521-549.
4. Demerouti, E., Bakker, A. B., Nachreiner, F., & Schaufeli, W. B. (2001). The job demands-resources model of burnout. *Journal of Applied Psychology*, 86(3), 499.
5. Furnell, S., & Thomson, K.-L. (2009). Recognising and addressing 'security fatigue'. *Computer Fraud & Security*, 2009(11), 7-11.
6. Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security fatigue. *IT Professional*, 18(5), 26-32.