International Journal of Multidisciplinary Research and Growth Evaluation.

Human Limits in Cyber Defence: Sleep, Stress, and Security Risk

Stephen Adeniyi Sobulo
University of Fairfax, USA

* Corresponding Author: **Stephen Adeniyi Sobulo**

Article Info

ISSN (Online): 2582-7138
Impact Factor (RSIF): 7.98
Volume: 06
Issue: 06
Received: 17-10-2025
Accepted: 20-11-2025
Published: 14-12-2025
Page No: 1229-1231

Abstract
The modern workspace puts Cybersecurity professionals under immense pressure. There are relentless cognitive and emotional demands on them in the discharge of their responsibilities, such as monitoring alerts, responding to incidents, and maintaining vigilance against ever-evolving threats. Therefore, adequate rest, which includes sufficient sleep, mental breaks, and downtime, is crucial for them to maintain the much-needed high levels of attention, decision-making, and creative problem-solving that this role demands. Conversely, rest deprivation precipitates cybersecurity fatigue, which leads to an increase in error rates, thereby undermining incident response and accelerating burnout and turnover.
This article reviews the importance of rest for sustaining cyber-defence capabilities. Additionally, it outlines the human-factors mechanisms by which fatigue degrades performance and proposes organizational strategies to embed recovery into security operations.

DOI: https://doi.org/10.54660/.IJMRGE.2025.6.6.1229-1231

Keywords: Cybersecurity Fatigue, Burnout, Sleep Deprivation, Stress, Performance Risk.

1. Introduction
The roles of cybersecurity professionals carry high stakes, because a single lapse can expose sensitive data, disrupt critical services, or endanger public safety. Therefore, these roles demand continuous vigilance, rapid threat analysis, and coordinated incident response. But human thought and emotion are limited resources, just like muscles. They need time to rest and recover to work at their best. Rest, which includes getting enough sleep, taking scheduled pauses, and mentally detaching, is not a luxury but a necessity that should be seen as a strategic advantage for cybersecurity operations.

2. Literature Review
2.1. Cybersecurity Fatigue and Its Impact
The constant exposure to complex security protocols, alerts, and compliance tasks often leads to exhaustion. This exhaustion is referred to as "Security fatigue" (Stanton *et al*., 2016) [13]. Nobles (2022) [7] identifies security fatigue as a human-factors problem that erodes both vigilance and morale, which results in higher error rates and a diminished security posture. In a survey of 351 employees across IT and other high-security sectors, researchers found that cybersecurity fatigue correlates strongly with increased stress and anxiety ($\rho = 0.56$, $p < .01$) and reduced productivity ($\rho = –0.41$, $p < .01$) (Mittu & Lawless, 2023) [4]. These findings point to the fact that chronic cognitive load from security tasks directly impairs both mental health and operational effectiveness.

2.2. Cognitive and Emotional Mechanisms
It has been established that rest supports executive functions, such as working memory, attention, and decision-making. It does this by consolidating learning and clearing metabolic byproducts in the brain (Walker, 2009) [14]. Conversely, sleep deprivation produces impairments on par with legal intoxication, degrading reaction times and judgment (Williamson & Feyer, 2000) [16].

In cybersecurity contexts, where rapid and accurate decisions are essential for incident triage and containment, even moderate fatigue can have significant consequences (Paul & Dykstra, 2017) [8].

Adequate rest functions as a critical protective factor against burnout among cybersecurity professionals, a condition characterized by emotional exhaustion, depersonalization, and reduced professional efficacy. Recent empirical and industry evidence indicates that burnout affects approximately 60–65% of security workers, with fatigue, excessive workload, and insufficient recovery time identified as key contributors (ISACA, 2024; Nepal *et al*., 2024) [3, 5]. Burnout significantly impairs crisis response capabilities, increases error rates, and heightens intentions to leave the profession, thereby accelerating attrition and the loss of institutional knowledge in a workforce already constrained by chronic skills shortages. These dynamics, in turn, inflate recruitment and onboarding costs while further destabilizing organizational security operations (ISC², 2024; Hack The Box, 2024) [17, 2].

2.3. Comparisons with IT Professionals Generally

Furthermore, broader studies of IT and knowledge workers corroborate these dynamics. Pilcher and Morris (2020) [10] demonstrated that poor sleep quality is associated with reduced workplace safety, increased errors, and lower creativity across various professions, including the IT sector. Similarly, Peng *et al*. (2023) [9] found that, among a sample of 487 employees, diminished sleep quality was significantly negatively related to occupational well-being and job satisfaction, mediated in part by reduced self-efficacy. These general IT findings suggest that the fundamental human factors influencing rest and performance are consistent across various technical domains; however, the stakes and stressors in cybersecurity often intensify these effects.

3. Consequences of Inadequate Rest

A lot of consequences of inadequate rest have been noted by research, such as:

1. **Increased Incident Response Failures:** Fatigued analysts can misclassify threats, delay containment, or misconfigure defences. These errors can exacerbate breaches and prolong recovery times (Reeves, Calic, & Delfabbro, 2020) [11].
2. **Accelerated Burnout and Turnover:** Chronic rest deprivation among cybersecurity professionals significantly contributes to emotional exhaustion, a core dimension of occupational burnout. Empirical and industry evidence indicate that burnout prevalence in security teams frequently reaches—and in some contexts exceeds—approximately 65%, particularly among incident responders and high-demand operational roles. Elevated burnout levels are consistently associated with increased turnover intentions and actual attrition, resulting in the loss of institutional knowledge that is critical for maintaining organizational security maturity. Moreover, burnout-driven attrition exacerbates workforce shortages, leading to higher recruitment, onboarding, and training costs, and thereby imposes substantial financial and operational burdens on organizations (Hack The Box, 2024; ISACA, 2024; Nepal *et al*., 2024; (ISC)², 2023) [2, 3, 5, 17].
3. **Diminished Strategic Innovation:** Creativity and strategic foresight, which are critical for anticipating adversary tactics, depend on insight processes that occur during sleep. Therefore, a lack of rest can hinder innovation in threat-hunting and defence design (Wagner *et al*., 2004) [15].
4. **Systemic Security Risks:** Organizations with fatigued security teams exhibit poorer patch management, vulnerability scanning, and policy enforcement, thereby creating exploitable gaps across critical infrastructure sectors (Aamoth, 2025) [1].

4. Recommendations for Embedding Rest in Cybersecurity Operations

1. **Structured Shift Rotations & Protected Breaks:** Develop duty roster models that restrict successive hours on alert systems and require periodic mental rest intervals throughout shifts.
2. **Sleep Hygiene & Shift Scheduling Education:** Offer training on circadian rhythms, pre-shift preparation, and post-shift recovery techniques to optimize sleep quality (Pilcher & Morris, 2020) [10].
3. **Digital Detox Protocols:** Implement post-incident "cool-down" periods, which are mandatory intervals devoid of security alerts, to facilitate cognitive recuperation and mitigate emotional aftereffects (Mittu & Lawless, 2023) [4].
4. **On-site Rest Facilities:** Provide quiet rooms or nap pods in security operations centres to enable short restorative breaks without compromising coverage.
5. **Mental Health Support:** Integrate counselling services and resilience training into the benefits of security teams, recognizing mental health as integral to mission readiness (Nobles, 2022) [7].

5. Conclusion

Rest underpins the cognitive sharpness, emotional resilience, and creative problem-solving that are essential for cybersecurity professionals. It has been confirmed that inadequate rest can lead to fatigue, increase error rates, and accelerate burnout that can compromise an organization's security posture. Implementing organized rest rules, informed by human-factors research and best practices from cybersecurity and general IT, enables firms to maintain high-performance, high-reliability teams essential for countering emerging threats.

6. References

1. Aamoth D. Report: addressing cybersecurity burnout in 2025. Sophos; 2025 Sep 30. Available from: https://news.sophos.com/en-us/2025/09/30/report-addressing-cybersecurity-burnout-in-2025/
2. Hack The Box. Building a firewall against cybersecurity burnout. Hack The Box Research; 2024. Available from: https://resources.hackthebox.com/building-a-firewall-against-cybersecurity-burnout
3. ISACA. State of cybersecurity 2024: global update on workforce trends. ISACA; 2024. Available from: https://www.isaca.org/resources/reports/state-of-cybersecurity-2024
4. Mittu R, Lawless WF. Digital detox: exploring the impact of cybersecurity fatigue on employee productivity and mental health. Discover Ment Health. 2023; doi: 10.1007/s44192-025-00149-x
5. Nepal S, Di Troia F, Stamp M, Greitzer FL. Burnout in cybersecurity incident responders. ACM Trans Priv

Secur. 2024;27(2):1-28. doi: 10.1145/3634737
6. Nepal S, Jansen A, Khurana S, Nurse JRC. Burnout in cybersecurity incident responders. Proc ACM Hum-Comput Interact. 2024;8(CSCW):Article 120. doi: 10.1145/3613904
7. Nobles C. Stress, burnout, and security fatigue in cybersecurity: a human factors problem. Holistica J Bus Public Adm. 2022;13(1):49-72. doi: 10.2478/hjbpa-2022-0003
8. Paul CL, Dykstra J. Understanding operator fatigue, frustration, and cognitive workload in tactical cybersecurity operations. J Inf Warf. 2017;16(2):1-11. Available from: https://www.jinfowar.com/journal/volume-16-issue-2/understanding-operator-fatigue-frustration-cognitive-workload-tactical-cybersecurity-operations
9. Peng J, Zhang Z, Wang D, He L, Lin X, Fang Y, *et al*. The relationship between sleep quality and occupational well-being in employees: the mediating role of occupational self-efficacy. Front Psychol. 2023;14:9911531. doi: 10.3389/fpsyg.2023.1071232
10. Pilcher JJ, Morris DM. Sleep and organizational behaviour: implications for workplace productivity and safety. Front Psychol. 2020;11:45. doi: 10.3389/fpsyg.2020.00045
11. Reeves A, Calic D, Delfabbro P. Sleeping with the enemy: does depletion cause fatigue with cybersecurity? In: HCI for cybersecurity, privacy and trust. Springer; 2020. p. 217-231. doi: 10.1007/978-3-030-50309-3_15
12. Sonnentag S, Binnewies CH, Parker SL. Recovery from work: advancing the field toward the future. Annu Rev Organ Psychol Organ Behav. 2022;9:33-60. doi: 10.1146/annurev-orgpsych-012420-091355
13. Stanton B, Theofanos MF, Prettyman S, Furman S. Security fatigue. IT Prof. 2016;18(5):26-32. doi: 10.1109/MITP.2016.84
14. Walker MP. The role of sleep in cognition and emotion. Ann N Y Acad Sci. 2009;1156(1):168-197. doi: 10.1111/j.1749-6632.2009.04416.x
15. Wagner U, Gais S, Haider H, Verleger R, Born J. Sleep inspires insight. Nature. 2004;427(6972):352-355. doi: 10.1038/nature02223
16. Williamson AM, Feyer AM. Moderate sleep deprivation produces impairments in cognitive and motor performance equivalent to legally prescribed levels of alcohol intoxication. Occup Environ Med. 2000;57(10):649-655. doi: 10.1136/oem.57.10.649
17. (ISC)². Cybersecurity workforce study 2023. ISC2; 2023. Available from: https://cybergovernancealliance.org/wp-content/uploads/2024/01/ISC2_Cybersecurity_Workforce_Study_2023-1.pdf
18. (ISC)². Cybersecurity workforce study 2024. International Information System Security Certification Consortium; 2024. Available from: https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

How to Cite This Article
Sobulo SA. Human limits in cyber defence: sleep, stress, and security risk. Int J Multidiscip Res Growth Eval. 2025;6(6):1229–1231. doi:10.54660/.IJMRGE.2025.6.6.1229-1231.