Exploring Mitigative Strategies to Prevent Burnout in Cybersecurity

Calvin Nobles
University of Maryland Global Campus, Adelphi, USA

Calvin.nobles@umgc.edu

Abstract: Burnout poses a critical challenge in cybersecurity, affecting both individual well-being and organizational effectiveness. Despite its importance, limited scholarly research exists on preventive strategies specific to cybersecurity, hindering the development of evidence-based approaches. Current literature predominantly examines the causes, constructs, and theoretical models of burnout in cybersecurity, with insufficient focus on preventing this occupation phenomenon. This study addresses this gap by synthesizing existing research to propose strategic initiatives to combat burnout among cybersecurity professionals. Key prevention strategies include dynamic prioritization frameworks, flexible work policies, role-specific interventions to balance workloads and alleviate stress, personalized recognition programs, resilience-oriented onboarding, and enhanced engagement and psychological readiness. Other vital initiatives include supportive workplace cultures, inclusive environments, leadership development, and access to mental health resources, which are critical for mitigating emotional exhaustion and depersonalization. This research highlights initiatives, emphasizing the urgent need for further research to fill the gap in burnout prevention strategies for cybersecurity. By adopting a multifaceted approach, organizations can foster resilience, enhance employee well-being, and strengthen their capacity to address complex challenges to develop mitigative strategies to prevent burnout in cybersecurity.

Keywords: Burnout, Cybersecurity, Fatigue, Human performance, Prevention, Stress

1. Introduction

The cybersecurity domain faces immense pressure due to the rapidly evolving nature of cyber threats, creating high-stakes environments requiring constant vigilance. This sustained stress, combined with increasingly complex security challenges, contributes to a heightened risk of burnout among cybersecurity professionals. Human risk factors, including stress, burnout, and security fatigue, must be effectively addressed to reduce an organization's vulnerability to cyber-attacks and security breaches (Nobles, 2022). Burnout, characterized by (a) emotional exhaustion, (b) depersonalization, and (c) a diminished sense of personal accomplishment, not only affects individual well-being but also compromises an organization's security resilience (Nobles, 2022).

According to Malasch and Schaufeli (2018), burnout has been widely recognized as a primary driver of workforce attrition, significantly undermining employee retention and organizational stability. Without a doubt, burnout adversely affects organizations and individuals that impede production or optimize operations. Researchers play a critical role in reframing the discourse on burnout within cybersecurity, shifting the focus from reactive responses to proactive mitigative strategies aimed at prevention. By advancing evidence-based insights and interventions, researchers can help organizations prioritize identifying and managing factors contributing to burnout, fostering a sustainable and resilient cybersecurity workforce. This paper aims to explore strategies to prevent burnout in cybersecurity.

This article is structured to thoroughly examine strategies for preventing burnout in cybersecurity. Section 2 lays the groundwork by defining burnout and its relevance to cybersecurity. Section 3 explores human performance issues as contributors to and outcomes of burnout. Section 4 examines the organizational and individual factors influencing burnout. Section 5 focuses on preventive measures tailored to the cybersecurity context. Section 6 provides actionable recommendations, while Section 7 concludes the discussion with key insights and future directions.

2. Defining Burnout

Burnout, first defined by Freudenberger (1974) and expanded by Maslach, is recognized in the ICD-11 as a syndrome resulting from unmanaged workplace stress (Bianchi & Schonfeld, 2023; Sharma & Cooper, 2016). It consists of emotional exhaustion, depersonalization, and reduced personal accomplishment, with symptoms varying by individual and organizational context (Bianchi & Schonfeld, 2023). Cybersecurity professionals face high stress due to constant threats, operational pressures, and increasing attack complexity. Research highlights that burnout significantly affects performance and well-being, with 85% of cybersecurity professionals reporting fatigue and stress (Naprys, 2024). The shift to remote work and rising nation-state cyber threats have worsened these challenges (Reeves et al., 2023). Unlike temporary stress, burnout becomes systemic, leading to reduced vigilance and security lapses (Naprys, 2024). Burnout arises from both organizational and individual factors, requiring a comprehensive approach. Workplace culture, leadership, and workload management influence stress levels, while individual resilience affects coping capacity (Sharma & Cooper, 2016). Despite its impact,

human performance issues in cybersecurity remain underexplored, underscoring the need for research-driven interventions to strengthen workforce resilience and security effectiveness.

3. Human Performance Issues in Cybersecurity

Stress, burnout, and cybersecurity fatigue remain pervasive challenges in the cybersecurity sector, exacerbated by leadership's failure to address their systemic causes (Nobles, 2022; Platsis, 2019). Despite their critical role in security resilience, human performance issues remain largely overlooked, leading organizations to rely on technological solutions that inadvertently increase operational complexity and "complexity debt" (Wilson, Hamilton, & Stallbaum, 2020). The lack of scholarly focus on human factors in cybersecurity further perpetuates this gap, hindering the development of effective mitigation strategies.

Human performance degradation is a major contributor to cybersecurity incidents, yet it remains one of the most underappreciated dimensions of organizational security (Wilson et al., 2020). Addressing this issue requires integrating cognitive, behavioral, and organizational factors into security strategies. Awareness and education programs significantly reduce breaches by training employees to recognize phishing attempts and social engineering tactics (Legrand, 2022; Salvagioni et al., 2017). Behavioral analysis, including monitoring for anomalous user activity, is critical for early threat detection (Moustafa et al., 2021). Additionally, designing security protocols around human limitations enhances compliance and reduces errors (Nobles & Robinson, 2023).

Error management strategies, such as regular audits, clear guidelines, and responsive support systems, help mitigate human errors, a leading cause of security breaches (Chaudhary et al., 2022). Moreover, fostering a strong security culture within organizations enhances collective defense mechanisms and reinforces best practices (Jesson et al., 2020). Continuous skill development ensures cybersecurity professionals can respond effectively to evolving threats, while structured workload management prevents burnout-induced errors and security lapses (Legrand, 2022). Without prioritizing human factors, organizations risk sustaining adverse behavioral patterns that increase vulnerability, reinforcing the urgent need for a holistic cybersecurity strategy.

4. Individual and Organizational Factors in Burnout

Burnout can be broadly categorized into two distinct dimensions, as outlined in Tables 1 and 2—organizational and individual factors. These dimensions encompass the primary contributors and underlying causes of burnout, providing a comprehensive understanding of its origins. Tables 1 and 2 illustrate critical organizational and individual factors contributing to burnout. While not exhaustive, these tables offer valuable insights into the multifaceted challenges organizations and individuals face in addressing and mitigating burnout.

Table 1: Organizational Factors Leading to Burnout

Factor Type	Specific Factors	Description	References
Organizational	High Workload	Excessive tasks and responsibilities with insufficient time or resources lead to chronic stress.	Maslach & Leiter (2016); Bakker & Demerouti (2017)
	Lack of Autonomy	Minimal control over work-related decisions, reducing employee engagement and increasing frustration.	Schaufeli & Bakker (2004); Kim & Wang (2018)
	Poor Leadership	Ineffective communication, lack of support, and unclear supervisor expectations cause employee strain.	Kahn et al. (2021); Skakon et al. (2010)
	Inadequate Recognition	Failure to acknowledge or reward employee contributions leads to feelings of undervaluation.	Maslach & Jackson (1981); Ducharme et al. (2008)
	Unfair Treatment	Perceived inequities in resource allocation or decision-making foster resentment and stress.	Greenberg (2006); Bakker et al. (2021)

Factor Type	Specific Factors	Description	References
	Workplace Conflict	Interpersonal tensions and lack of team cohesion create a stressful and unproductive work environment.	De Dreu & Weingart (2003); Leiter & Maslach (2009)
	Insufficient Resources	Lack of tools, training, or support to meet job demands exacerbates stress.	Hobfoll (2001); Demerouti et al. (2001)

Burnout in the workplace is often driven by organizational factors that place undue strain on employees, eroding their well-being and productivity. High workloads, characterized by excessive responsibilities and insufficient resources, cause chronic stress in professional settings. Maslach and Leiter (2016) emphasize that unrelenting workloads deplete energy levels and diminish job satisfaction and commitment. Similarly, Bakker and Demerouti (2017) highlight that organizations failing to provide adequate time or tools for task completion exacerbate employee exhaustion. The lack of autonomy further intensifies these challenges; Schaufeli and Bakker (2004) argue that minimal control over work-related decisions reduces engagement and fosters frustration. Poor leadership, characterized by ineffective communication and unclear expectations, intensifies employee strain, as highlighted by Kahn et al. (2021), who emphasize the essential role of supportive supervisors in alleviating workplace stress.

Table 2: Individual Factors Leading to Burnout

Factor Type	Specific Factors	Description	References
Individual	Perfectionism	Unrealistic self-expectations and an overcommitment to work result in self-imposed stress.	Hill et al. (2018); Shoss (2017)
	Inability to Detach	Difficulty disconnecting from work during off-hours, leading to prolonged exposure to stress.	Sonnentag & Fritz (2015); Derks et al. (2014)
	Low Resilience	Limited capacity to recover quickly from stress or adversity, increasing vulnerability to burnout.	Tugade & Fredrickson (2004); Shirom (2003)
	Poor Time Manaagement	Ineffective prioritization and organization of tasks contribute to chronic stress and reduced efficiency.	Macan (1994); Claessens et al. (2007)
	Work-life Balance	Disproportionate focus on work at the expense of personal life, leading to emotional exhaustion.	Allen et al. (2000); Carlson et al. (2010)
	Emotional Exhaustion	Persistent feelings of fatigue and depletion caused by excessive work demands.	Maslach et al. (2001); Bakker et al. (2014)
	Negative Coping Mechanism	Use of unhealthy strategies, such as avoidance or substance use, to handle stress.	Aldao et al. (2010); Folkman & Moskowitz (2004)

Individual factors also play a significant role in the development of burnout, particularly when combined with organizational stressors. Perfectionism, for example, imposes unrealistic expectations and leads to self-imposed stress, as Hill et al. (2018) noted. This tendency is exacerbated by an inability to detach from work during off-hours, which prolongs exposure to stressors and prevents recovery. Sonnentag and Fritz (2015) demonstrate that individuals who cannot mentally disconnect from their professional responsibilities are more likely to experience chronic stress and emotional exhaustion. Emotional exhaustion, a hallmark of burnout, manifests as persistent fatigue and depleted energy levels, impairing an individual's ability to meet job demands effectively (Maslach et al., 2001; Bakker et al., 2014). These factors illustrate the complex interplay between personal behaviors and workplace conditions in the burnout phenomenon.

The organizational environment can further amplify the impact of individual vulnerabilities through systemic issues such as insufficient recognition and workplace conflict. Failing to acknowledge employee contributions undermines morale and fosters feelings of undervaluation, as highlighted by Maslach and Jackson (1981). Similarly, interpersonal tensions and a lack of team cohesion create a toxic environment that inhibits productivity and increases stress, according to De Dreu and Weingart (2003). Addressing burnout requires a dual approach: organizations must prioritize allocating adequate resources, implement supportive leadership practices, and foster a collaborative culture, while individuals must adopt strategies to enhance resilience and improve work-life balance. A holistic understanding of both organizational and individual factors, supported by interventions at both levels, is essential to mitigate burnout and sustain a productive, engaged workforce.

5. Correlation of Burnout From Existing Studies

Burnout in cybersecurity is a critical risk factor, directly impairing vigilance, decision-making, and adherence to security protocols. Shain and Kramer (2020) found that burned-out employees exhibit reduced cognitive function, making them more susceptible to phishing and cyber threats. Similarly, D'Arcy et al. (2021) identified burnout as a key driver of security violations, as fatigued employees neglect protocols. Security compliance burnout, where excessive security demands lead to disengagement, further exacerbates these vulnerabilities (D'Arcy et al., 2014; Pham et al., 2019). Lee et al. (2017) reinforced that burnout erodes awareness and weakens security decision-making, underscoring the urgency of integrating burnout mitigation into cybersecurity programs.

Burnout not only degrades performance but also escalates security risks. Nepal et al. (2024) found that burned-out security professionals disengage, reducing vigilance and increasing breach likelihood. High turnover worsens staffing shortages, forcing reliance on less experienced teams ill-equipped to handle cyber threats. The Job Demands-Resources model explains how excessive workloads without adequate support impair cognition and resilience, weakening security postures (Nepal et al., 2024). Sleep deprivation and cognitive fatigue further hinder decision-making, while burnout-induced disengagement leads to lapses in attention and compliance (Dreison et al., 2018). Schaufeli and Enzmann (1998) highlighted that burnout diminishes moral responsibility, reducing employees' commitment to critical security practices under stress. The link between burnout and cybersecurity vulnerabilities is well-documented—organizations that fail to address burnout risk increased security breaches, human errors, and operational instability. Proactively mitigating burnout strengthens resilience, reduces cyber threats, and ensures a more secure workforce.

6. De-Isolating Burnout

Burnout in cybersecurity is not an isolated phenomenon but rather a systemic issue driven by organizational, technological, and psychological factors that collectively impact security effectiveness. High job demands—such as complex threat mitigation, incident response pressures, and constant vigilance—exacerbate burnout, particularly when paired with inadequate leadership support, insufficient training, and ineffective security tools (Pham et al., 2019). The Job Demands-Resources model illustrates how excessive workloads without adequate coping mechanisms create a feedback loop where burnout depletes cognitive resources, weakens security performance, and perpetuates further stress (Bakker & Demerouti, 2017). Additionally, security compliance burnout emerges when employees feel overwhelmed by rigid security policies, excessive monitoring, and unrealistic compliance expectations, leading to disengagement and policy negligence (D'Arcy et al., 2014). This underscores that burnout is an individual concern and an organizational challenge influenced by leadership, workplace culture, and security policies.

Beyond structural factors, individual resilience, cognitive capacity, and emotional intelligence shape employees' ability to manage stress and maintain cybersecurity effectiveness. Employees with strong coping mechanisms are more resistant to burnout, while those with lower resilience are prone to emotional exhaustion, impairing their ability to detect and respond to threats (Lee et al., 2017). Cognitive overload from constant exposure to cyber threats, information fatigue, and multitasking further intensifies burnout, increasing susceptibility to errors and social engineering attacks (Dreison et al., 2018). External stressors, such as work-life imbalance and mental health struggles, compound these risks, making a multidimensional intervention necessary. Organizations must go beyond surface-level solutions and integrate workload management, psychological support systems, and workplace culture reforms to prevent burnout's cascading impact on cybersecurity resilience (Kivimäki et al., 2002).

7. Preventing Burnout in Cybersecurity

Burnout remains a pervasive challenge in cybersecurity, with 55% of professionals frequently experiencing work-related stress and 28% of CISOs at risk of leaving their roles due to burnout (Oltsik, 2023). This phenomenon poses significant risks to both individual well-being and organizational resilience, amplifying vulnerabilities in an already high-pressure field (Nobles, 2022; Reeves et al., 2024). Burnout develops gradually, underscoring the necessity of adopting preventive measures tailored to individual and organizational needs.

Existing literature underscores the growing impact of burnout on individuals and organizations in cybersecurity. Despite its critical importance, there is a notable gap in scholarly research focused on preventive strategies specific to cybersecurity. This lack of research limits the ability of organizations and individuals to develop evidence-based approaches to mitigate burnout effectively in cybersecurity. Most existing studies primarily explore the causes, constructs, and theoretical models of burnout in cybersecurity rather than actionable solutions. Table 3 highlights strategic initiatives derived from the limited studies on burnout in cybersecurity, emphasizing the urgent need for more targeted research to address this pressing issue. The following table organizes the identified preventive measures into broader themes with corresponding descriptions and sources. This thematic grouping highlights actionable insights for preventing burnout among cybersecurity professionals.

Table 3: Mitigation Strategies to Combat Burnout

Strategic Initiative	Description	References
Workplace Flexibility	Promoting flexible work arrangements, including remote work, adjustable hours, and boundaries, supports work-life balance and reduces stress.	Ajayi & Udeh (2024); Huarng (2001); Nepal et al. (2024); Reeves et al. (2024)
Leadership and Recognition	Encouraging transformational leadership, personalized recognition initiatives, and appreciation programs that boost morale, satisfaction, and engagement.	Ajayi & Udeh (2024); Nepal et al. (2024); Huarng (2001)
Supportive Culture	Fostering an inclusive and collaborative environment with mentorship, team-building activities, and open communication to address emotional exhaustion and build mutual support among employees.	Reeves et al. (2021); Ajayi & Udeh (2024); Nepal et al. (2024); Huarng (2001)
Cognitive Load Management	Reducing cognitive demands by aligning complex tasks with low-stress periods, simplifying workflows, and addressing decision fatigue through intuitive design and optimized processes.	Reeves et al. (2021); Pham et al. (2019); Nepal et al. (2024)
Training and Development	Implementing tailored training programs, onboarding resilience strategies, and job-specific interventions to build skills and prepare employees for cybersecurity's psychological demands.	Huarng (2001); Reeves et al. (2021); Nepal et al. (2024)
Monitoring and Assessment	Regularly evaluate well-being using structured tools like the CyFa framework, identify fatigue sources, and implement targeted interventions to address systemic and individual stressors.	Pittas et al. (2024); Ajayi & Udeh (2024); Nepal et al. (2024)
Workload Management	Utilizing dynamic prioritization frameworks, proactive workload assessments, and effective project management practices to balance tasks and minimize stress.	Nepal et al. (2024); Huarng (2001)
Mental Health Resources	Providing access to counseling, mindfulness programs, wellness technologies, and resilience training to address stress and promote well-being.	Ajayi & Udeh (2024); Nepal et al. (2024); Reeves et al. (2024)
Policy and Systemic Changes	Developing policies that address systemic stressors, such as excessive workloads and role ambiguity, while safeguarding employee privacy and embedding burnout prevention in organizational practices.	Pittas et al. (2024); Reeves et al. (2024); Nepal et al. (2024)
Diversity and Inclusion	Promoting gender diversity, equitable treatment, and measures to eliminate cultural barriers, creating a supportive environment for underrepresented groups.	Reeves et al. (2024); Pittas et al. (2024)
Technology Integration	Leveraging apps and tools to monitor stress and wellness, designing human-centered systems to enhance engagement, and simplifying security requirements to align with employee capabilities.	Ajayi & Udeh (2024); Pham et al. (2019); Reeves et al. (2021)
Sleep Quality Improvements	Addressing poor sleep through manageable shift schedules, breaks, and work-life integration strategies to mitigate emotional exhaustion and improve recovery.	Reeves et al. (2024)

A central approach involves addressing workloads and task management. Nepal et al. (2024) advocate for dynamic prioritization frameworks that adapt tasks based on responders' expertise and emotional states, ensuring efficiency without overburdening employees. Similarly, Huarng (2001) highlights the importance of effective project management practices to align resources with timelines, preventing excessive demands on team members. Regular monitoring and assessment of workloads, as emphasized by both Nepal et al. (2024) and Ajayi and Udeh (2024), can preempt capacity issues and distribute tasks more equitably.

Creating supportive workplace cultures also plays a critical role in preventing burnout. Structured team-building activities, mentorship programs, and open communication foster collaboration and mutual support during high-stress periods and are foundational to combatting burnout (Ajayi & Udeh, 2024; Nepal et al., 2024). These efforts can mitigate feelings of isolation and depersonalization, commonly associated with burnout (Huarng, 2001). Reeves et al. (2024) emphasize the importance of inclusive work environments that promote diversity and equitable treatment, particularly for underrepresented groups, to reduce cultural barriers and feelings of alienation.

Flexible work policies and personalized recognition initiatives reduce stress and enhance job satisfaction. Ajayi and Udeh (2024) highlight the role of remote work options, flexible hours, and clear boundaries in achieving work-life integration. Personalized appreciation programs, including non-monetary rewards, further boost motivation and engagement (Nepal et al., 2024). When combined with investments in staffing and training, these strategies ensure that employees are well-equipped to meet role-specific challenges without undue strain.

Training and professional development are critical components of burnout prevention. Nepal et al. (2024) propose resilience-oriented onboarding processes that include stress management techniques to prepare employees for the psychological demands of cybersecurity roles. Similarly, targeted training programs on stress management and effective communication can help employees navigate interpersonal and role-specific challenges (Huarng, 2001).

The integration of mental health resources and technological solutions further supports employee well-being. Access to counseling, mindfulness programs, and wellness technologies, such as wearable devices for stress monitoring, are practical interventions (Ajayi & Udeh, 2024). Reeves et al. (2021) emphasize the need to reduce cognitive load through intuitive system designs and simplified cybersecurity processes, aligning organizational requirements with employee capacities. Systemic and policy-level changes are essential for sustaining these efforts. Organizations must address structural stressors, such as role ambiguity and workload imbalances, while safeguarding employee privacy in burnout monitoring initiatives (Nepal et al., 2024; Pittas et al., 2024). Comprehensive policy revisions that prioritize systemic solutions over individual blame foster a healthier work environment and reduce burnout risks (Pittas et al., 2024).

Combating burnout in cybersecurity requires a multifaceted approach combining workload management, supportive culture, flexibility, mental health resources, and systemic change. By implementing these strategies, organizations can foster a resilient and engaged workforce, ultimately enhancing individual well-being and organizational effectiveness.

8. Burnout and Human Performance

Many people in cybersecurity suffer from prolonged and high levels of stress, fatigue, and distraction (Nobles, 2022). While suffering from the human performance issues above does not indicate burnout, the diagnosis must come from a physician, not a self-diagnosis. Without a doubt, cybersecurity professionals experiencing stress, fatigue, or other ailments should seek immediate attention but refrain from self-diagnosis. Burnout occurs from long exposure to high stress levels and fatigue (Nobles, 2022). While cybersecurity professionals could perform their duties while facing stress and fatigue, this is not an optimal or prudent condition, given the intricate duties of some cybersecurity professionals. Wilson et al. (2020) indicate that human performance degradation is a real phenomenon in cybersecurity. Human performance degradation (Wilson et al., 2020) and increasing stress levels, fatigue, and distractions (Nobles, 2022) illustrate that cybersecurity professionals work under less-than-optimal conditions. These conditions make cybersecurity professionals prone to errors (Wilson et al., 2022), and most cybersecurity breaches result from human-induced errors (Nobles, 2022). This highlights the adverse effects of extensive exposure to stress, fatigue, and burnout.

Based on the studies listed in Table 1, the researchers did not isolate burnout from other occupational and psychological stressors that may contribute to its onset. However, it is well-established that burnout does not emerge suddenly but rather develops over time due to sustained exposure to workplace stress and chronic fatigue (Maslach & Leiter, 2016). Attempting to isolate burnout as a distinct construct can provide a clearer

understanding of its unique antecedents and consequences, facilitating targeted interventions (Schaufeli et al., 2009). However, such an approach also risks oversimplifying the complex interplay between burnout and other mental health conditions, such as depression and anxiety, which often co-occur (Bianchi et al., 2015). Furthermore, workplace factors—including organizational culture, leadership style, and job demands—contribute to burnout in ways that may not be fully understood if studied in isolation (Demerouti et al., 2001). Therefore, while isolating burnout may enhance conceptual clarity, a more holistic approach that acknowledges its multifaceted nature may yield deeper insights into its causes and potential solutions.

The cybersecurity sector is increasingly recognizing the detrimental effects of burnout on professionals' performance and overall organizational security. While some individuals may maintain baseline operational duties despite experiencing burnout, research indicates that their capacity to manage complex security challenges diminishes significantly. Burnout is associated with cognitive impairments, including decreased attention, memory, and problem-solving skills, which are crucial for effective cybersecurity operations. A study by Nobles (2022) highlights that stress, burnout, and security fatigue continue to undermine robust cybersecurity practices, emphasizing the need for organizations to address these human factors proactively. Furthermore, a survey conducted by Arora and Hastings (2024) revealed that 44% of cybersecurity professionals report severe work-related stress and burnout, with an additional 28% uncertain about their condition. This pervasive issue affects individual well-being and compromises the organization's ability to respond effectively to evolving cyber threats. Therefore, while some professionals may temporarily uphold standard security protocols despite burnout, the associated cognitive decline and reduced engagement present significant risks to cybersecurity resilience.

9. Recommendations

Preventing burnout in cybersecurity requires a strategic, research-driven approach that prioritizes human performance issues (stress, fatigue, and burnout) and addresses the unique stressors in this field. Empirical studies highlight heightened emotional exhaustion and inefficacy among cybersecurity professionals, necessitating targeted interventions. Integrating human factors practitioners into cybersecurity teams can optimize workflows, reduce cognitive overload, and enhance decision-making, addressing critical performance issues.

Fatigue management practices, such as structured breaks, workload rotation, and adaptive scheduling, are essential for maintaining alertness in high-pressure environments. Additionally, in cybersecurity, interventions must reflect the nuanced demands of specific roles, tailoring resilience training, mental health support, and recognition programs to fit the needs of cybersecurity professionals working in various roles.

Organizations must also invest in empirical research to close gaps in understanding burnout in cybersecurity. Collaborative efforts with interdisciplinary teams can create robust frameworks that align technical and human factors. Cybersecurity organizations can sustain workforce well-being and resilience in the face of escalating demands by addressing fatigue, customizing interventions, and fostering a supportive environment.

10. Conclusion

Preventing burnout in cybersecurity is essential to safeguarding both workforce well-being and organizational effectiveness in a high-stress, high-demand industry. Research highlights unique stressors, including emotional exhaustion and cognitive overload, yet the lack of targeted studies limits evidence-based interventions. Integrating human factors practices, such as designing workflows and systems aligned with human capabilities and implementing fatigue management strategies like structured breaks and adaptive scheduling, are critical for sustaining performance. Tailored approaches, including role-specific resilience training, personalized recognition programs, and accessible mental health resources, address the diverse needs across cybersecurity roles. Furthermore, investing in interdisciplinary research is vital to bridging knowledge gaps and creating robust, adaptive frameworks. By prioritizing proactive and customized strategies, organizations can foster a resilient workforce equipped to meet the complex challenges of cybersecurity while maintaining individual and organizational well-being. For future consideration, more research is necessary to understand the manifestation of burnout in cybersecurity and the need to identify prevention strategies derived from empirical inquiries.

References

Ajayi, F. A., & Udeh, C. A. (2024). Combating burnout in the IT Industry: A review of employee well-being initiatives. *International Journal of Applied Research in Social Sciences*, *6*(4), 567-588.

Aldao, A., Nolen-Hoeksema, S., & Schweizer, S. (2010). Emotion-regulation strategies across psychopathology: A meta-analytic review. *Clinical Psychology Review, 30*(2), 217-237.

Allen, T. D., Herst, D. E. L., Bruck, C. S., & Sutton, M. (2000). Consequences associated with work-to-family conflict: A review and agenda for future research. *Journal of Occupational Health Psychology, 5*(2), 278.

Arora, S., & Hastings, J. D. (2024). A survey-based quantitative analysis of stress factors and their impacts among cybersecurity professionals. *arXiv preprint arXiv:2409.12047*.

Bakker, A. B., Demerouti, E., & Sanz-Vergel, A. I. (2014). Burnout and work engagement: The JD–R approach. *Annual Review of Organizational Psychology and Organizational Behavior, 1*(1), 389-411.

Bakker, A. B., & Demerouti, E. (2017). Job demands–resources theory: Taking stock and looking forward. *Journal of Occupational Health Psychology, 22*(3), 273–285.

Bianchi, R., Schonfeld, I. S., & Laurent, E. (2015). Burnout–depression overlap: A review. *Clinical Psychology Review, 36*, 28–41.

Bianchi, R., & Schonfeld, I. S. (2023). Examining the evidence base for burnout. *Bulletin of the World Health Organization*, *101*(11), 743–745. https://doi.org/10.2471/BLT.23.289996

Carlson, D. S., Kacmar, K. M., & Williams, L. J. (2000). Construction and initial validation of a multidimensional measure of work–family conflict. *Journal of Vocational Behavior, 56*(2), 249–276.

Claessens, B. J. C., van Eerde, W., Rutte, C. G., & Roe, R. A. (2007). A review of the time management literature. *Personnel Review, 36*(2), 255-276.

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal of Cybersecurity*, *8*(1), tyac006.

D'Arcy, J., Hovav, A., & Galletta, D. F. (2014). User adherence to information security policies: The role of social influence. *Information Systems Research*, 25(1), 10-26.

D'Arcy, J., Hovav, A., & Galletta, D. (2021). Employee burnout and cybersecurity behavior: A dual process model. *Information Systems Research*, 32(3), 827-845.

De Dreu, C. K. W., & Weingart, L. R. (2003). Task versus relationship conflict, team performance, and team member satisfaction: A meta-analysis. *Journal of Applied Psychology, 88*(4), 741-749.

Demerouti, E., Bakker, A. B., Nachreiner, F., & Schaufeli, W. B. (2001). The job demands-resources model of burnout. *Journal of Applied Psychology, 86*(3), 499-512.Derks, D., van Mierlo, H., & Schmitz, E. B. (2014). A diary study on work-related smartphone use, psychological detachment, and exhaustion: Examining the role of the perceived segmentation norm. *Journal of Occupational Health Psychology, 19*(1), 74-84.

Dreison, K. C., Luther, L., Bonfils, K. A., Sliter, M. T., McGrew, J. H., & Salyers, M. P. (2018). Job burnout in mental health providers: A meta-analysis of 35 years of intervention research. *Journal of Occupational Health Psychology*, 23(1), 18-30.

Derks, D., van Mierlo, H., & Schmitz, E. B. (2014). A diary study on work-related smartphone use, psychological detachment, and exhaustion: Examining the role of the perceived segmentation norm. *Journal of Occupational Health Psychology, 19*(1), 74-84.

Ducharme, L. J., Knudsen, H. K., & Roman, P. M. (2008). Emotional exhaustion and turnover intention in human service occupations: The protective role of coworker support. *Sociological Spectrum, 28*(1), 81-104.

Dykstra, J., & Paul, C. L. (2018). Cyber Operations Stress Survey (COSS): Studying fatigue, frustration, and cognitive workload in cybersecurity operations. In *11th USENIX Workshop on Cyber Security Experimentation and Test CSE, 18*.

Eaton, L. (2019). Health workforce burnout. *World Health Organization. Bulletin of the World Health Organization*, *97*(9), 585-586.

Folkman, S., & Moskowitz, J. T. (2004). Coping: Pitfalls and promise. *Annual Review of Psychology, 55*, 745-774.

Greenberg, J. (2006). Losing sleep over organizational injustice: Attenuating insomniac reactions to underpayment inequity with supervisory training in interactional justice. *Journal of Applied Psychology, 91*(1), 58-69.

Hill, A. P., Curran, T., & Hall, H. K. (2018). Perfectionism in sport, dance, and exercise: An extended review and re-analysis. *International Review of Sport and Exercise Psychology, 12*(1), 1-34.

Hobfoll, S. E. (2001). The influence of culture, community, and the nested-self in the stress process: Advancing conservation of resources theory. *Applied psychology*, *50*(3), 337-421.

Huarng, A. S. (2001). Burnout Syndrome among Information System Professionals. *Inf. Syst. Manag.*, *18*(2), 1-6.

Kahn, W. A., Barton, M. A., & Fellows, S. (2021). Organizational crises and the disturbance of relational systems. *Academy of Management Review, 46*(3), 456-474.

Kävrestad, J., & Naqvi, B. (2024, July). Cognitively Available Cybersecurity: A Systematic Literature Review. In *International Conference on Human-Centred Software Engineering* (pp. 160-170). Cham: Springer Nature Switzerland.

Kim, T., & Wang, J. (2018). Work-life imbalance and burnout among working mothers in Korea: A cultural expectation perspective. *International Journal of Human Resource Management, 29*(15), 2208-2233.

Lee, J., Kim, J., & Lee, J. (2017). The effect of emotional intelligence on information security compliance: The mediating effects of cybersecurity awareness and burnout. *Computers in Human Behavior*, 66, 205-212.

Legrand, J. (2022). Humans and Cybersecurity—The Weakest Link or the Best Defense? ISACA Journal.

Leiter, M. P., & Maslach, C. (2009). Nurse turnover: The mediating role of burnout. *Journal of Nursing Management, 17*(3), 331-339.

Macan, T. H. (1994). Time management: Test of a process model. *Journal of Applied Psychology, 79*(3), 381-391.

Maslach, C., & Jackson, S. E. (1981). The measurement of experienced burnout. *Journal of Occupational Behavior, 2*(2), 99-113.

Maslach, C., & Leiter, M. P. (2016). Understanding the burnout experience: Recent research and its implications for psychiatry. *World Psychiatry, 15*(2), 103–111.

Maslach, C., & Schaufeli, W. B. (2018). Historical and conceptual development of burnout. In *Professional Burnout* (pp. 1-16). CRC Press.

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. *Frontiers in Psychology*, *12*, 561011.

Naprys, E. (2024). Hidden crisis in cybersecurity: 17 out of 20 professionals suffering from fatigue and burnout. Cybernews. https://cybernews.com/security/hidden-crisis-cybersecurity-professionals-suffering-from-burnout/

Nepal, S., Hernandez, J., Lewis, R., Chaudhry, A., Houck, B., Knudsen, E., ... & Czerwinski, M. (2024). Burnout in Cybersecurity Incident Responders: Exploring the Factors that Light the Fire. *Proceedings of the ACM on Human-Computer Interaction*, *8*(CSCW1), 1-35.

Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *HOLISTICA–Journal of Business and Public Administration*, *13*(1), 49-72.

Nobles, C., & Robinson, N. (2024). 3 The benefits of human factors engineering in cybersecurity. *Cybersecurity Risk Management: Enhancing Leadership and Expertise*, 53.

Oltsik, J. (2023, July). The life and time of cybersecurity professionals, Vol 6. https://www.issa.org/wp-content/uploads/2023/08/ESG-eBook-ISSA-2023.pdf

Pallardy, R. (2024, February 22). The psychology of cybersecurity burnout. https://www.informationweek.com/cyber-resilience/the-psychology-of-cybersecurity-burnout

Pham, H. C., Brennan, L., & Furnell, S. (2019). Information security burnout: Identification of sources and mitigating factors from security demands and resources. *Journal of Information Security and Applications*, *46*, 96-107.

Pittas, D., Delfabbro, P., & Reeves, A. (2024). How to De-CyFa the actor-observer bias in cybersecurity fatigue: Building the CyFa measure of attribution styles and mitigation strategies. *Computers & Security*, 104179.

Platsis, G. (2019, August 14). Is staff burnout the best reason to implement cybersecurity A.I.? Securityintelligence.com. Retrieved from https://securityintelligence.com/articles/is-staff-burnout-the-best-reason-to-implement-cybersecurity-ai/

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *SAGE open*, *11*(1), 21582440211000049.

Reeves, A., Pattinson, M., & Butavicius, M. (2023, July). Is your CISO burnt out yet? Examining demographic differences in workplace burnout amongst cyber security professionals. In *International Symposium on Human Aspects of Information Security and Assurance* (pp. 225-236). Cham: Springer Nature Switzerland.

Reeves, A., Pattinson, M., & Butavicius, M. (2024). The sleepless sentinel: factors that predict burnout and sleep quality in cybersecurity professionals. *Information & Computer Security*, 46, 96-107.

Salvagioni, D. A. J., Melanda, F. N., Mesas, A. E., González, A. D., Gabani, F. L., & Andrade, S. M. D. (2017). Physical, psychological and occupational consequences of job burnout: A systematic review of prospective studies. *PloS one*, *12*(10), e0185781.

Schaufeli, W. B., & Enzmann, D. (1998). *The burnout companion to study and practice: A critical analysis*. London: Taylor & Francis

Schaufeli, W. B., & Bakker, A. B. (2004). Job demands, job resources, and their relationship with burnout and engagement: A multi-sample study. *Journal of Organizational Behavior, 25*(3), 293–315.

Schaufeli, W. B., Leiter, M. P., & Maslach, C. (2009). *Burnout: 35 years of research and practice Career Development International, 14 (3), 204-220*.

Shain, M. & Kramer, L. (2020). Burnout and Attention to Cybersecurity. *Journal of Cybersecurity Research*, 8(2), 45-61.

Sharma, R. R., & Cooper, S. C. (2016). *Executive burnout: Eastern and Western concepts, models, and approaches for mitigation*. Emerald Group Publishing Limited.

Shirom, A. (2003). Job-related burnout: A review. *Handbook of Occupational Health Psychology*, 245-264.

Singh, T., Johnston, A. C., D'Arcy, J., & Harms, P. D. (2023). Stress in the cybersecurity profession: A systematic review of related literature and opportunities for future research. *Organizational Cybersecurity Journal: Practice, Process and People*, *3*(2), 100-126.

Skakon, J., Nielsen, K., Borg, V., & Guzman, J. (2010). Are leaders' well-being, behaviours and style associated with the affective well-being of their employees? A systematic review of three decades of research. *Work & Stress, 24*(2), 107-139.

Sonnentag, S., & Fritz, C. (2015). Recovery from job stress: The stressor-detachment model as an integrative framework. *Journal of Organizational Behavior, 36*(1), S72–S103.

Tugade, M. M., & Fredrickson, B. L. (2004). Resilient individuals use positive emotions to bounce back from negative emotional experiences. *Journal of Personality and Social Psychology, 86*(2), 320-333.

Wilson, S., Hamilton, & Stallbaum, S. (2020, May 26). The unaddressed gap in cybersecurity: Human performance. *MIT Sloan Management Review*. Retrieved from https://sloanreview.mit.edu/article/the-unaddressed-gap-in-cybersecurity-human-performance/