

Burnout: A Hidden Cybersecurity Risk

Burnout is often overlooked in cybersecurity conversations, yet it poses a substantial threat to an organization's security posture. It not only affects the well-being of employees but also impairs their ability to remain alert, make sound decisions, and follow established security protocols. Burnout can stem from both workplace demands and external life stress, both of which increase the risk of human error—the most common cause of data breaches.

Burnout from Work: The Known Risk

Cybersecurity professionals and IT teams often operate under immense pressure. They work long hours, handle high-stakes responsibilities, and are expected to respond quickly to emerging threats—all of which contribute to professional burnout.

- A **2024 1Password report** revealed that **84% of cybersecurity professionals** experience burnout, and **65%** admit it has affected their ability to perform critical security tasks.
- **ISACA's 2023 State of Cybersecurity Report** found that **52% of cybersecurity teams** are understaffed, often leading to overwork, high stress, and more frequent mistakes.
- Burnout has also been linked to **higher insider threat risk**, with **Gartner (2024)** reporting that it contributed to a **30% rise in negligent insider security incidents**.

Burnout from Life: The Overlooked Threat

Burnout isn't always caused by work. Personal stress—such as financial worries, caregiving responsibilities, illness, or mental health struggles—can also take a toll on cognitive performance. These issues may be invisible in the workplace but still have a major impact on employee behavior.

- A **2024 Gallup poll** reported that **44% of employees** feel stressed daily, citing personal life issues as major contributors.
- The **2023 Deloitte Workplace Burnout Survey** found that **nearly 70% of professionals** believe their employer does not adequately support work-life balance, further intensifying stress levels.

- According to the **2024 Mental Health Foundation (UK)**, **61% of employees** said personal stress impairs their concentration and decision-making at work—two key faculties in maintaining cybersecurity awareness.

Security Consequences of Burnout

Whether caused by work or life outside of it, burnout can lead to serious cybersecurity vulnerabilities:

- **Increased Likelihood of Human Error**
Tired, distracted employees are more prone to mistakes such as clicking phishing links, misconfiguring systems, or sending data to the wrong recipient.
- **Decreased Policy Adherence**
Employees under stress may begin to see security protocols as burdensome and start bypassing or ignoring them—for example, disabling MFA, using weak passwords, or skipping software updates.
- **Weakened Threat Response**
A burned-out team is less responsive to real-time threats. When energy and motivation are low, response times slow, and incident detection becomes inconsistent.
- **Greater Attrition in Security Roles**
High turnover due to burnout creates knowledge gaps and weakens continuity. Replacing experienced professionals is costly and introduces new risks during onboarding.

Building a Burnout-Resilient Culture

Combatting burnout requires a strategic, whole-person approach. It's not enough to manage workloads—organizations must create an environment where mental health and balance are prioritized:

- **Promote Work-Life Balance**
Offer flexible work schedules, remote work opportunities, and adequate paid time off to help employees manage personal responsibilities without sacrificing productivity.
- **Support Mental Wellbeing**
Provide access to employee assistance programs (EAPs), counseling, and wellness platforms. Normalize conversations about mental health.

- **Encourage Breaks and Recovery Time**

Create a culture that values breaks, boundaries, and recovery—especially after stressful incidents such as breach responses or audits.

- **Foster Psychological Safety**

Allow employees to express when they are overwhelmed or struggling, without fear of judgment. Managers should be trained to respond supportively.

- **Distribute Security Responsibility**

Spread cybersecurity responsibilities across roles and departments so no one person or small team bears the full burden.

- **Monitor for Signs of Burnout**

Be proactive. Use anonymous surveys, one-on-one check-ins, and feedback loops to identify early signs of burnout and address them before they lead to errors.

The Bottom Line

Burnout—whether fuelled by workplace conditions or personal life stress—directly increases cybersecurity risk. Employees who are overworked, distracted, or emotionally drained are significantly more likely to make critical mistakes, ignore threats, or disengage from security practices altogether.

Organizations that take proactive steps to support mental health, reduce stress, and build a culture of balance are not only investing in their people—they're strengthening their first line of cyber defense.

References

- ❑ 1Password (2021) *The Burnout Breach Report*. Available at: <https://1password.com/resources/2021-state-of-secure-access-report/> (Accessed: 2 April 2025).[1Password+11passwordstatic.com+1](https://1password.com/resources/2021-state-of-secure-access-report/)
- ❑ ISACA (2023) *New ISACA Research: 59 Percent of Cybersecurity Teams are Understaffed*. Available at: <https://www.isaca.org/about-us/newsroom/press-releases/2023/new-isaca-research-59-percent-of-cybersecurity-teams-are-understaffed> (Accessed: 2 April 2025).[ISACA](https://www.isaca.org/about-us/newsroom/press-releases/2023/new-isaca-research-59-percent-of-cybersecurity-teams-are-understaffed)
- ❑ Gartner (n.d.) *Cybersecurity Leaders Are Burned Out. Here's Why*. Available at: <https://www.gartner.com/en/articles/cybersecurity-leaders-are-burned-out-here-s-why> (Accessed: 2 April 2025).[Gartner](https://www.gartner.com/en/articles/cybersecurity-leaders-are-burned-out-here-s-why)

- 2 Gallup (2023) *State of the Global Workplace Report*. Available at: <https://www.gallup.com/workplace/349484/state-of-the-global-workplace.aspx> (Accessed: 2 April 2025).[Gallup.com+1](#)[Gallup.com+1](#)
- 2 Deloitte (n.d.) *Workplace Burnout Survey*. Available at: <https://www2.deloitte.com/us/en/pages/about-deloitte/articles/burnout-survey.html> (Accessed: 2 April 2025).[Deloitte](#)
- 2 Mental Health Foundation (n.d.) *Stress: Statistics*. Available at: <https://www.mentalhealth.org.uk/explore-mental-health/statistics/stress-statistics> (Accessed: 2 April 2025).[Mental Health Foundation+1](#)[Mental Health Foundation+1](#)
- 2 ASIS International (2025) *Tackling Burnout in the High-Stakes World of Security*. Available at: <https://www.asisonline.org/security-management-magazine/articles/2025/01/burnout/tackling-burnout/> (Accessed: 2 April 2025).[ASIS International](#)
- 2 Gallup (2024) *The Post-Pandemic Workplace: The Experiment Continues*. Available at: <https://www.gallup.com/workplace/657629/post-pandemic-workplace-experiment-continues.aspx> (Accessed: 2 April 2025).[Gallup.com](#)
- 2 Deloitte (2023) *Gen Z and Millennial Survey*. Available at: <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/deloitte-2023-genz-millennial-survey.pdf> (Accessed: 2 April 2025).[Deloitte+1](#)[Deloitte+1](#)
- 2 Mental Health Foundation (n.d.) *Mental Health at Work: Statistics*. Available at: <https://www.mentalhealth.org.uk/explore-mental-health/statistics/mental-health-work-statistics> (Accessed: 2 April 2025).[Mental Health Foundation+1](#)[Mental Health Foundation+1](#)
-