SOPHOS

THE HUMAN COST OF VIGILANCE: ADDRESSING CYBERSECURITY BURNOUT IN 2025

A Sophos Whitepaper. August 2025

Introduction

The cybersecurity landscape is increasingly defined by the unrelenting pressure of sophisticated cyber threats, including ransomware. This pervasive threat environment places immense demands on IT and cybersecurity teams, leading to a significant and growing challenge: cybersecurity fatigue and burnout.

This report examines the direct human impact of these pressures, drawing on new research data to reveal the prevalence, key drivers, and consequences of burnout, ultimately underscoring how strategic solutions can mitigate this critical issue.

Data was collected via a vendor-agnostic survey of 5,000 IT and cybersecurity professionals across 17 countries. The survey took place in the first quarter of 2025 and asked respondents to reflect on their experiences over the course of the previous 12 months.

Understanding cybersecurity fatigue and burnout

Cybersecurity fatigue is characterized[1] by a state of mental and emotional exhaustion, often stemming from constant vigilance, alert overload, and the high-stakes nature of defending against evolving cyber threats. It signifies the cognitive and emotional drain experienced by professionals in this demanding field.

Burnout, a more generalized psychological syndrome, encompasses emotional exhaustion, cynicism, and a reduced sense of personal accomplishment, frequently as a result of chronic workplace stress. Within the cybersecurity domain, fatigue can be seen as a direct manifestation or a significant contributing factor to broader burnout.

Cybersecurity burnout is a specific manifestation of this broader burnout theory within the unique context of the cybersecurity field. It encompasses the mental, physical, and emotional exhaustion caused by excessive and prolonged exposure to the inherent stresses of cybersecurity work.

Professionals in this domain face unique cognitive and emotional demands, including the constant management of security alerts, the imperative to ensure compliance with stringent regulations, and the rapid response required for emerging cyber threats.

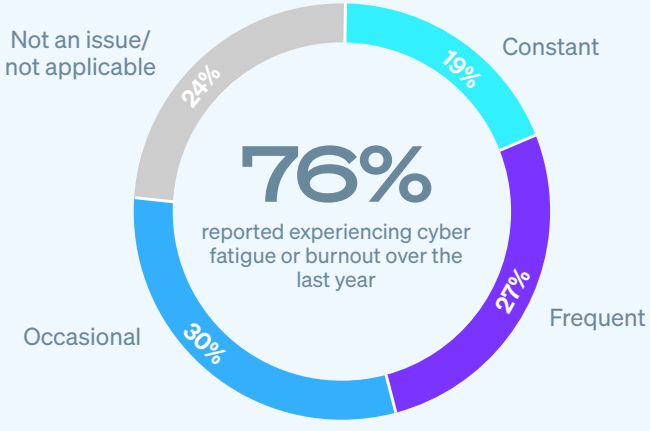
This continuous exposure to high-pressure tasks and the need for rapid, accurate responses to incidents are fundamental elements that amplify the risk of both fatigue and burnout within the cybersecurity workforce.

Pervasive strain and extensive repercussions

Experiences of burnout

The strain on cybersecurity professionals is evident in the widespread repercussions experienced by IT and cybersecurity teams over the past year.

When asked about personal experiences of cyber fatigue or burnout, 76% of respondents reported experiencing it themselves over the last year. Breaking it down further we see that 19% reported it being a “constant” issue, 27% reported it being a “frequent” issue, and 30% reported it being an “occasional” issue.



Have you experienced cybersecurity fatigue or burnout in the last year? n=5,000

The data reveals that burnout is a pervasive issue independent of organization size: 76% of respondents in businesses with 100-1,000 employees, 77% of respondents in businesses with 1,001-3,000 employees, and 75% of respondents in businesses with 3,001-5,000 employees experienced burnout.

What’s more, the problem is getting worse:
69% of respondents said cybersecurity fatigue and burnout increased from 2023 to 2024.

[1]Digital detox: exploring the impact of cybersecurity fatigue on employee productivity and mental health

The consequences of burnout

Unsurprisingly, burnout has significant negative impacts on the individuals that experience it, with almost half (46%) reporting heightened anxiety about cyberattacks or breaches, four in ten (39%) admitting to reduced productivity at work, and a third (33%) saying they have had a reduced level of engagement at work.

Consequences of cybersecurity fatigue and burnout

Impact of burnout	Average (n=3,803)	Level of burnout experienced		
		Constant issue (n=944)	Frequent issue (n=1,357)	Occasional issue (n=1,502)
Experienced heightened anxiety about cyberattacks or breaches	**46%**	47%	45%	46%
Reduced productivity at work	**39%**	36%	36%	43%
Reduced level of engagement at work	**33%**	34%	33%	34%
Needed to take time off work	**29%**	31%	28%	28%
Considered switching to a different career/role	**23%**	29%	25%	17%
Considered resigning from my/their job	**22%**	28%	25%	16%

What have been the personal consequences of the cyber fatigue or burnout, if any? Respondents that reported experiencing burnout in the previous 12 months. Base numbers in chart.

These figures highlight a pervasive challenge that directly undermines the effectiveness and sustainability of cybersecurity defenses.

Core causes of strain

The demanding nature of modern cyber defense, exacerbated by the relentless pace of cyberattacks, contributes significantly to burnout. Across all respondents who reported experiences of cyber fatigue or burnout, constant changes in cyber defense technologies/solutions was the most common contributing factor (38%). For those for whom burnout is a "constant" issue, the nature of cybersecurity work i.e., routine tasks interspersed with focused activities, is the most common cause, cited by 40% of respondents.

Factors causing cybersecurity fatigue and burnout

Cause of burnout	Average (n=3,803)	Level of burnout experienced		
		Constant issue (n=944)	Frequent issue (n=1,357)	Occasional issue (n=1,502)
Constant changes in cyber defense technologies/ solutions	**38%**	36%	37%	41%
The nature of cybersecurity work (routine tasks interspersed with focused activity)	**37%**	40%	36%	36%
Constant changes in threats	**34%**	31%	31%	39%
The need for 24/7 coverage	**32%**	30%	32%	33%
Pressure from changing regulatory and legal obligations	**32%**	34%	34%	29%
Constantly changing priorities	**30%**	28%	29%	32%
Pressure from board and/or executive management	**30%**	29%	30%	30%
Shortage of trained staff	**27%**	24%	26%	29%
Budget restrictions (excluding staffing)	**26%**	27%	28%	24%
Lack of access to expert third-party support	**26%**	30%	25%	23%
High volume of alerts	**25%**	24%	26%	25%

What factors were the cause of the cyber fatigue/burnout you experienced? Respondents that reported experiencing burnout in the previous 12 months. Base numbers in chart.

On average, respondents cited three separate factors that contributed to them experiencing burnout, highlighting the multiple pressures that IT teams face.

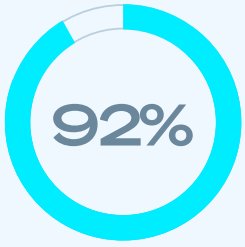
Individual and organizational impact

Unaddressed burnout has cascading negative effects, impacting both the individual well-being of security professionals and the overall resilience of the organization.

- **Individual impact:** Professionals suffer from heightened stress, anxiety, diminished job satisfaction, and adverse effects on their mental and physical health. This can also strain personal relationships and lead to increased turnover.
- **Organizational impact:**
  - Increased vulnerability: Exhausted teams are more prone to errors and oversights, potentially leading to critical security gaps and increased risk of successful breaches.
  - Reduced effectiveness: Burnout negatively impacts focus, decision-making, and productivity, compromising the team's ability to defend against advanced threats.
  - Talent attrition: The high stress associated with the role contributes to a churn of skilled professionals, exacerbating the existing cybersecurity talent shortage.
  - Operational disruption: A compromised security posture due to burnout can lead to more frequent and impactful security incidents, including ransomware attacks, resulting in operational downtime and significant financial losses.

Strategic measures and their effectiveness

Organizations are deploying various strategies to mitigate cybersecurity fatigue. While a range of internal measures are beneficial – such as fostering a supportive culture, providing mental health resources, and investing in professional development – the adoption of strategic external partnerships, particularly managed detection and response (MDR) services, shows significant promise.



of impacted respondents that use MDR say it reduced cybersecurity fatigue and burnout.

The research reveals that MDR services are a highly effective way to alleviate burnout, with 92% of impacted respondents that use a service saying it has reduced cybersecurity fatigue and burnout. Among those for whom burnout is a “constant” issue, half report a “significant” reduction and a further 45% saying the service has “somewhat” reduced burnout. This indicates a strong consensus that offloading critical security operations to expert MDR providers substantially reduces the pressure on internal teams.

Effectiveness of MDR services in reducing cybersecurity fatigue and burnout

Impact	Average (n=3,750)	Level of burnout experienced		
		Constant issue (n=940)	Frequent issue (n=1,340)	Occasional issue (n=1,470)
Significantly reduced burnout	**39%**	50%	35%	34%
Somewhat reduced burnout	**53%**	45%	56%	56%
Total	**92%**	95%	92%	90%

If your organization uses a managed detection and response (MDR) service, has it helped reduce experiences of cybersecurity fatigue or burnout? Respondents that reported experiencing burnout in the previous 12 months and whose organization uses an MDR service. Base numbers in chart.

Sophos MDR as a pillar of sustainable defense

The fight against cybercrime is relentless. To build a truly resilient defense, organizations must not only enhance their technological capabilities but also safeguard the well-being of their human defenders.

Sophos MDR offers a compelling solution to alleviate cybersecurity burnout by addressing many of the foundational causes:

- **Constant learning:** The Sophos MDR team is deeply attuned to innovations in both cyber defense technologies and threats, ensuring customers enjoy the full benefit of technology developments to optimize their defenses.
- **Continuous monitoring and immediate attack response:** Sophos MDR's expert analysts take care of the unpredictable nature of security operations for customers. From continuous monitoring, detection, and investigation tasks that consume significant bandwidth to full-scale threat response in the event of an incident that removes the (often out-of-hours) scramble for in-house teams.
- **Direct access to security experts:** Sophos MDR customers can call on the expertise of hundreds of analysts across all areas of security operations, including threat hunting, detection, investigation, and response specialists and behind-the-scenes malware and threat actor experts.
- **24/7 coverage:** Seven global security operations centers deliver seamless coverage, ensuring customers are fully protected at any time of the day or night.
- **AI-powered alert triage:** The sheer volume of security alerts can easily become overwhelming. Sophos MDR combines bespoke AI-powered triage tools with deep human expertise to enable us to quickly identify suspicious activities among the noise.

By partnering with Sophos MDR, organizations can establish a robust, proactive security posture that not only strengthens defenses against threats like ransomware but also critically supports the mental and professional well-being of their cybersecurity professionals, ensuring a sustainable and effective human defense in the face of evolving cyber threats.

Learn more about ransomware and how Sophos can help you defend your organization.

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

2025-08-26 WP (MP)

SOPHOS