SOCURA

Sleepless in security

Wellbeing in cyber and the challenges keeping security leaders awake at night.

Introduction

Now with nearly 84,000 professionals across the UK*, cyber security is a critical function essential to keeping the nation and businesses secure. However, the high-stakes nature of the profession can place a heavy strain on the individuals responsible for ensuring our ongoing defence against threats.

To understand the extent of these pressures and the impact they have on individuals' wellbeing and performance, Socura surveyed more than 500 security leaders.

In **Sleepless in security**, you'll learn about the physical and mental health issues executives experience, alongside the specific challenges keeping them awake at night. The report also explores attitudes towards the use of artificial intelligence and identifies factors that can improve employee satisfaction and retention.

* Source: A wave in cyber, employment trends report, Socura 2025

Contents

01. Key findings

Based on a survey of over 500 cyber security leaders in the UK

01 8 in 10 security leaders believe working in cyber has negatively impacted either their mental or physical health, with over a third taking formal leave due to stress.

02 Half of security leaders experience a nightmare or stressful work-related dream at least once a month.

03 42% of security leaders admit that stress significantly impacts their performance, with 86% worried that they could be fired in the event of a serious incident.

04 On average, security leaders work an extra 38 days a year in overtime, with three-quarters feeling a 'very large' or 'large' obligation to be contactable at all times.

05 Keeping pace with new threats, monitoring security posture 24/7 and governing AI use are among the top challenges cited by security leaders.

06 Despite the challenges of the role, 94% of cyber security leaders would recommend a career in the industry.

02. Methodology

In April 2026, Socura commissioned an online survey of 502 UK-based cyber security leaders. The survey was limited to professionals holding any of the following titles:

- Chief Security Officer
- Chief Information Security Officer
- Head of Information Security
- Director of Information Security
- IT Security Manager

Atomik Research, an independent research firm, conducted the survey in accordance with the Market Research Society Code of Conduct, ensuring respondent protection, data security, and compliance with UK GDPR and the Data Protection Act 2018.

03. The scale of stress and burnout in cyber

One of the chief aims of the survey was to better understand how working in cyber security impacts the physical and mental health of security leaders. This first section of the report explores the scale of these health challenges, as well as the common side effects that leaders experience as a result of stress and burnout.

3.1 Impact on physical and mental health

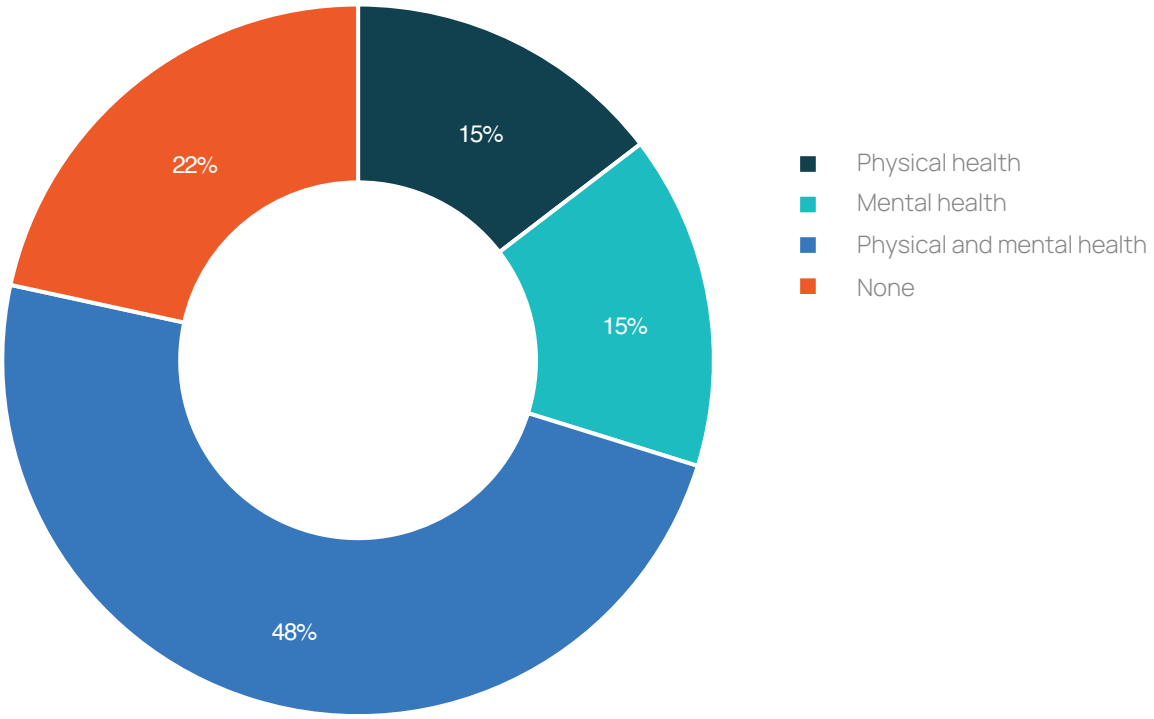
Alarmingly, nearly eight out of ten cyber security leaders surveyed (78%) reported that working in the industry has negatively impacted either their physical or mental health.

Nearly half of all respondents (48%) stated they had suffered both physical and mental issues as a result of working in the field.

8 in 10 security leaders believe working in cyber has negatively impacted their mental or physical health

03. The scale of stress and burnout in cyber

Do you believe working in cyber security has ever negatively impacted your physical and mental health?



While the physical and mental toll of working in cyber security won't come as a surprise to those inside the industry, the sheer extent to which cyber security leaders are suffering in their roles is undoubtedly a major cause for concern.

Factors contributing to security leaders' levels of stress are explored in section 6.

> Nearly half of security leaders have suffered both physical and mental issues as a result of work

03. The scale of stress and burnout in cyber

3.2 Common symptoms of stress

For security leaders experiencing physical and mental health impacts, we sought to identify specific symptoms. From a curated list, we asked security leaders to specify which symptoms they had experienced in the last 12 months due to work.

The most common symptom, reported by a quarter of respondents (25%), was a lack of sleep. Other common symptoms reported included social withdrawal, anxiety, and increased substance use. 13% of respondents stated that work had caused or contributed to depression.

28%
Feeling burnt out or exhausted

24%
Lack of sleep/ insomnia

23%
Social withdrawal

18%
Anxiety

18%
Increased substance use

13%
Depression

03. The scale of stress and burnout in cyber

3.3 Nightmares about work

Not only is a lack of sleep the most common negative health symptom experienced by security leaders, but the survey also found that the job impacts the quality of that sleep.

8 out of 10 security leaders have experienced at least one work-related dream in the last 12 months

Half of cyber security leaders (51%) say that they have a nightmare or stressful dream about work at least once per month

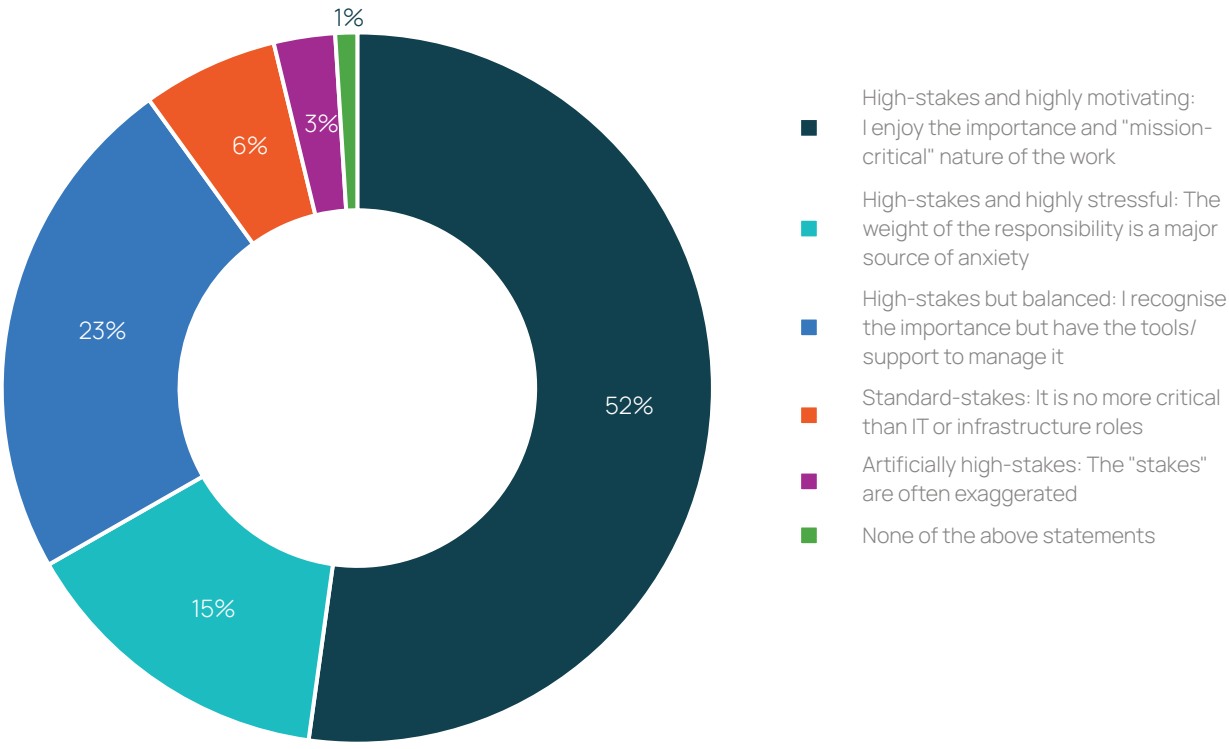
04. A high-stakes profession

Despite the physical and mental toll of working in cyber security, it's encouraging that security leaders recognise and value the importance of their work.

90% of survey respondents said that cyber security is a high-stakes field, with 52% of those describing the work as 'high-stakes and motivating'. 15% of those who view the industry as high-stakes described it as 'high-stakes and highly stressful.'

6% of overall respondents said that working in cyber security is no more critical than IT or infrastructure roles.

Which of the following best describes your personal perspective on the 'high-stakes' nature of a career in cyber security?



90% of security leaders consider working in cyber security as 'high stakes'

05. The root causes of stress

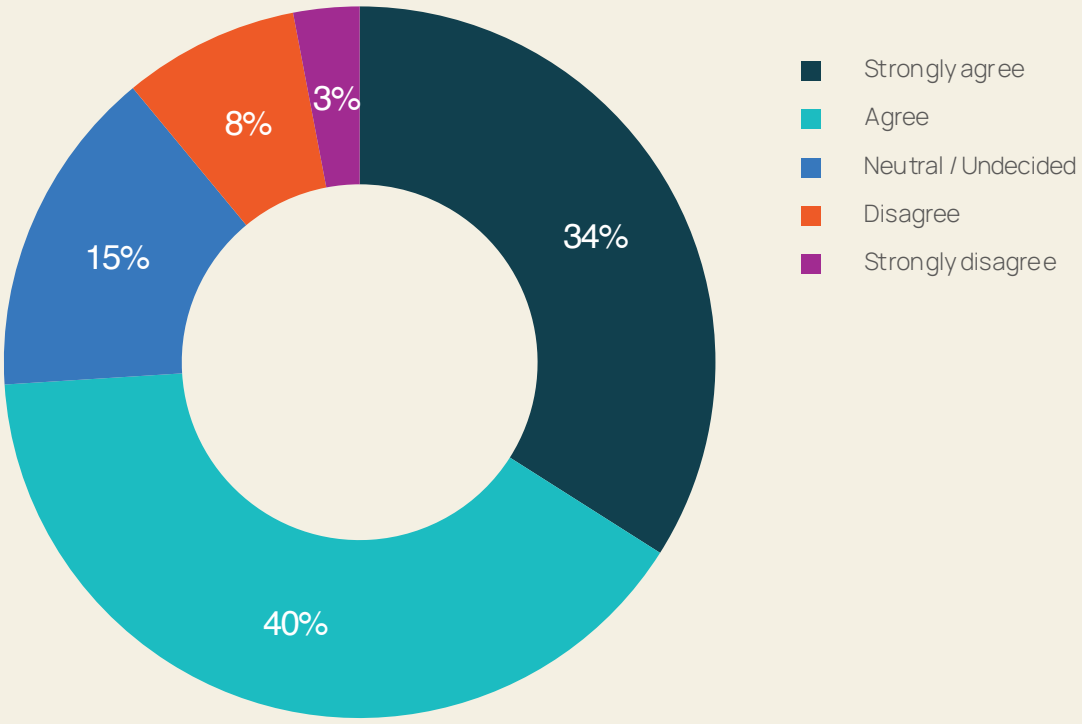
Despite an explosive growth in cyber security professionals over the last five years, a great amount of day-to-day pressure remains placed on security leaders. To gauge what is driving stress levels, the survey examined the compounding impacts of mounting workloads, systemic overtime, and the persistent weight of job insecurity.

5.1 Workload

Cyber security is a fast-paced industry. In order to understand the extent to which leaders struggle to keep up with their daily to-do list, we asked them how strongly they agree with the following statement: “I have too much to do, and not enough time to do it.”

Three-quarters of cyber security professionals 'strongly agreed' or 'agreed' that they had too much to do and not enough time to do it. While this feeling may not be uncommon across other industries, it is undoubtedly a revealing statistic about how security leaders feel about their workload, and helps to explain why so many feel the role impacts their physical and mental health.

How much do you agree: "I have too much to do, and not enough time to do it?”

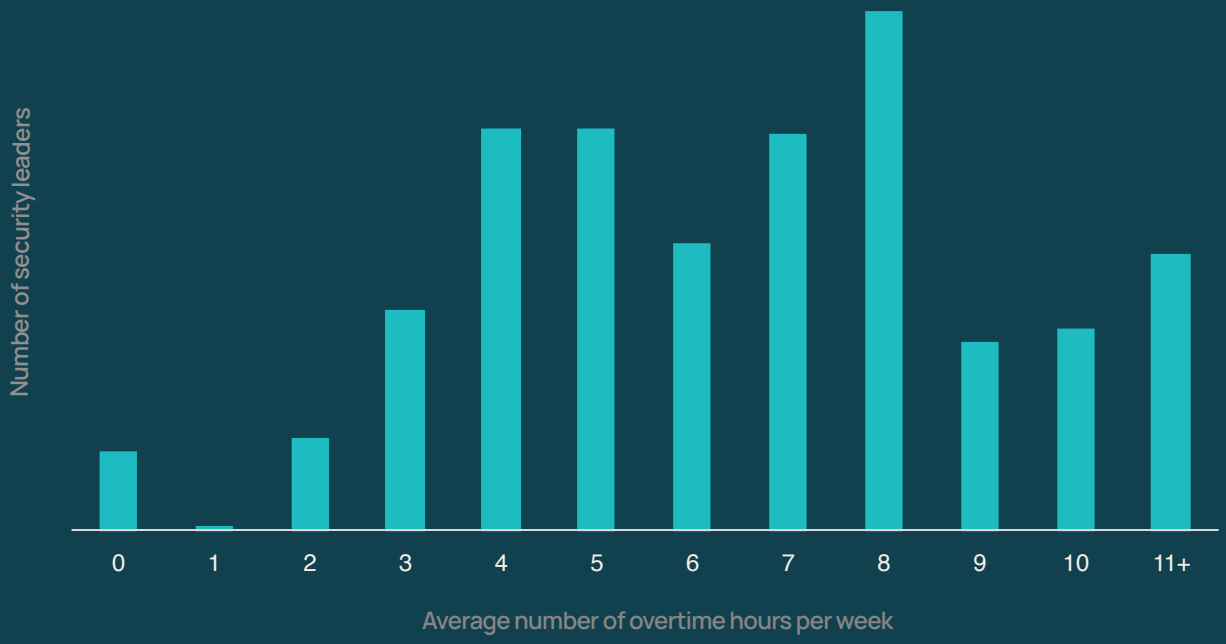


05. The root causes of stress

5.2 Overtime

Because of the relentless, high-stakes demands of cyber security, it is not uncommon for security leaders to work overtime and be on call, especially during highly demanding periods—such as in the aftermath of a serious incident or when critical vulnerabilities are disclosed.

Our survey found that the mean overtime for a cyber security leader is 6.5 additional hours per week (paid and unpaid). This figure equates to an extra 38 working days per year.*



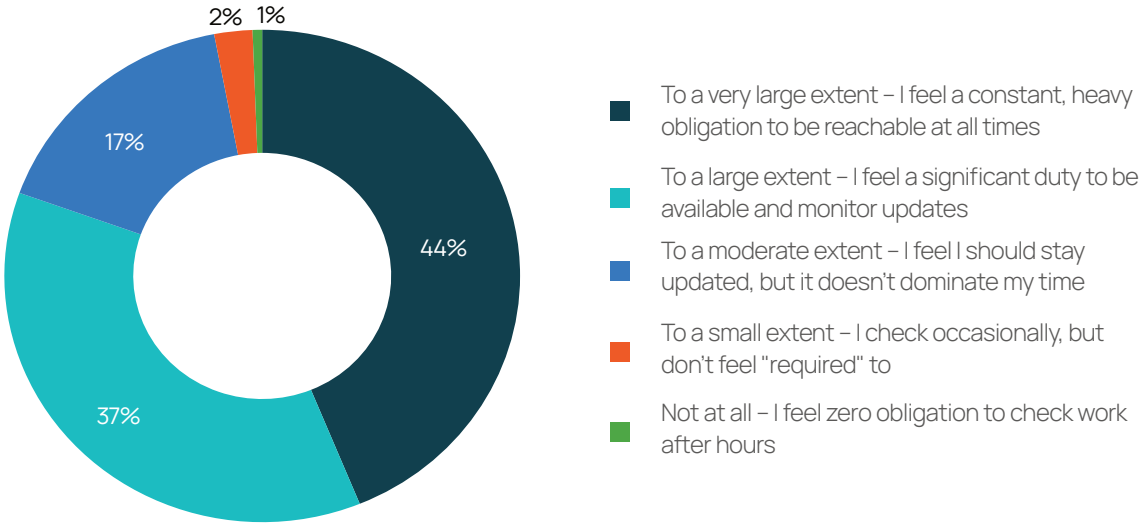
> The average security leader works an extra 38 days per year in overtime

* Figure based on a working day of eight hours and a security leader working 47 weeks per calendar year

05. The root causes of stress

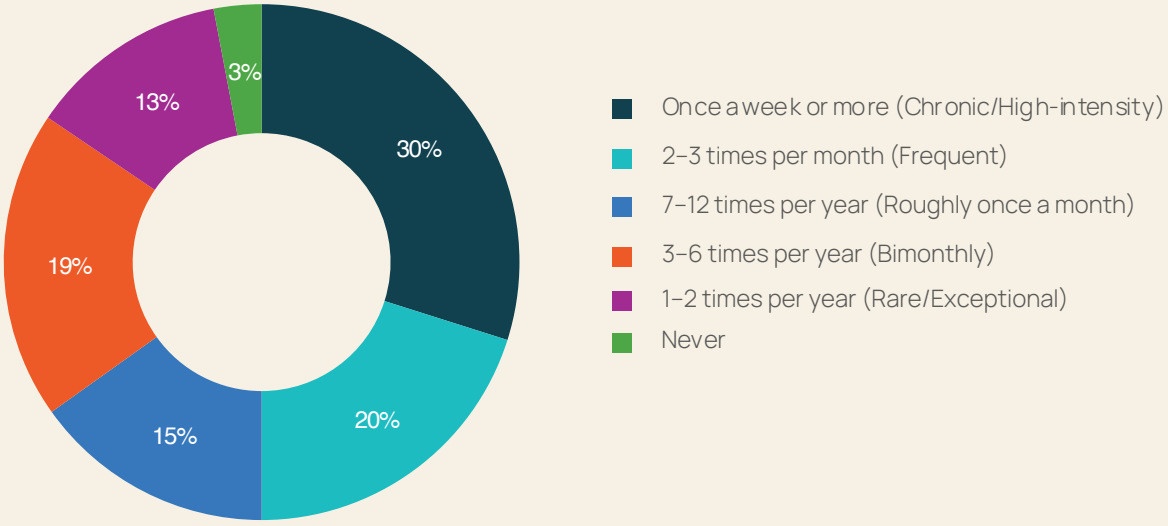
Three-quarters of cyber security leaders feel a 'very large' or 'large' obligation to monitor work communications and alerts outside of their contracted hours.

To what extent do you feel obliged to monitor work communications or alerts outside of your contracted hours?



The feeling security leaders have that they must be "always on" goes beyond just checking emails; 65% of workers have been called out or alerted out of hours due to a cyber security incident once a month or more. Nearly a third of senior cyber security professionals (30%) are called out at least once a week.

On average, in the last 12 months, how often have you been called out/ alerted after hours due to a cyber incident?



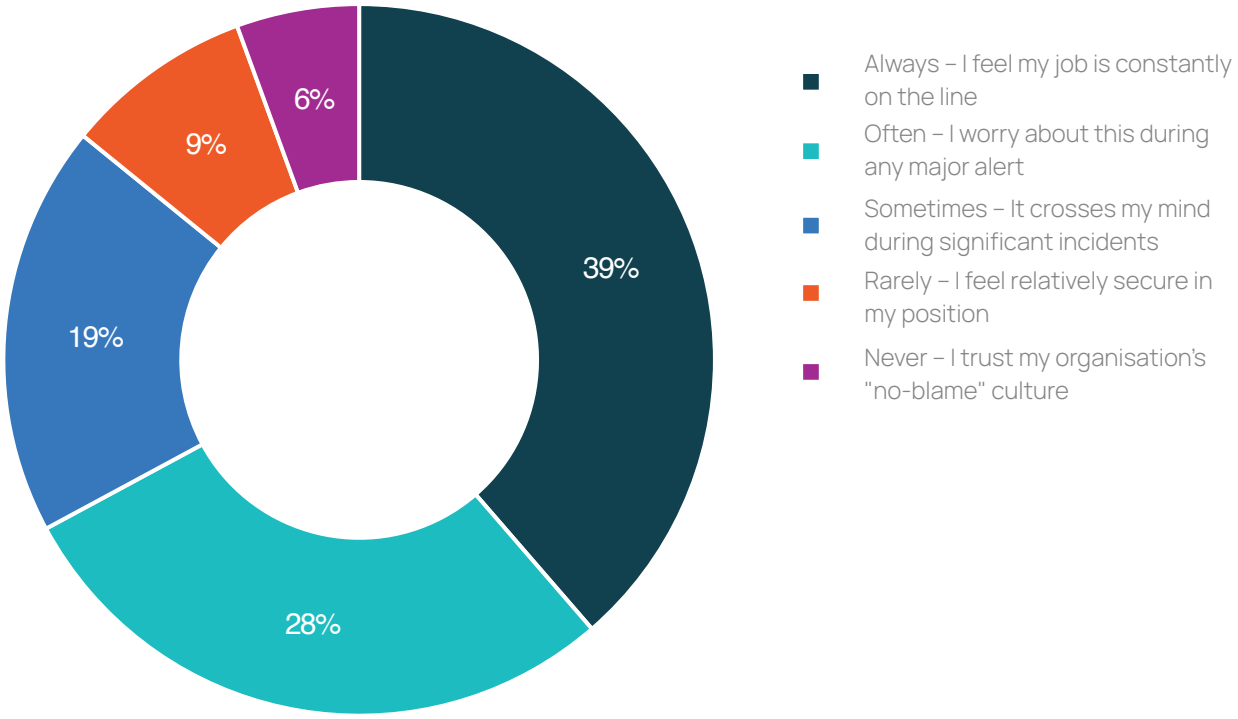
05. The root causes of stress

5.3 Job insecurity

Cyber incidents can be highly damaging to an organisation's finances and reputation. The survey found that security leaders shoulder a massive amount of the pressure to protect organisations against attacks, with 86% saying they always, often or sometimes worry about being fired in the event of a serious security incident.

Specifically, 39% of respondents said they "always" worry about the risk of being dismissed, 28% worry "often," and 19% worry "sometimes" during significant incidents.

Do you worry that you might get fired if there is a serious cyber security incident at your workplace?



> 86% of security leaders say they are concerned that they could be fired in the event of a serious cyber incident

06. The impact of stress

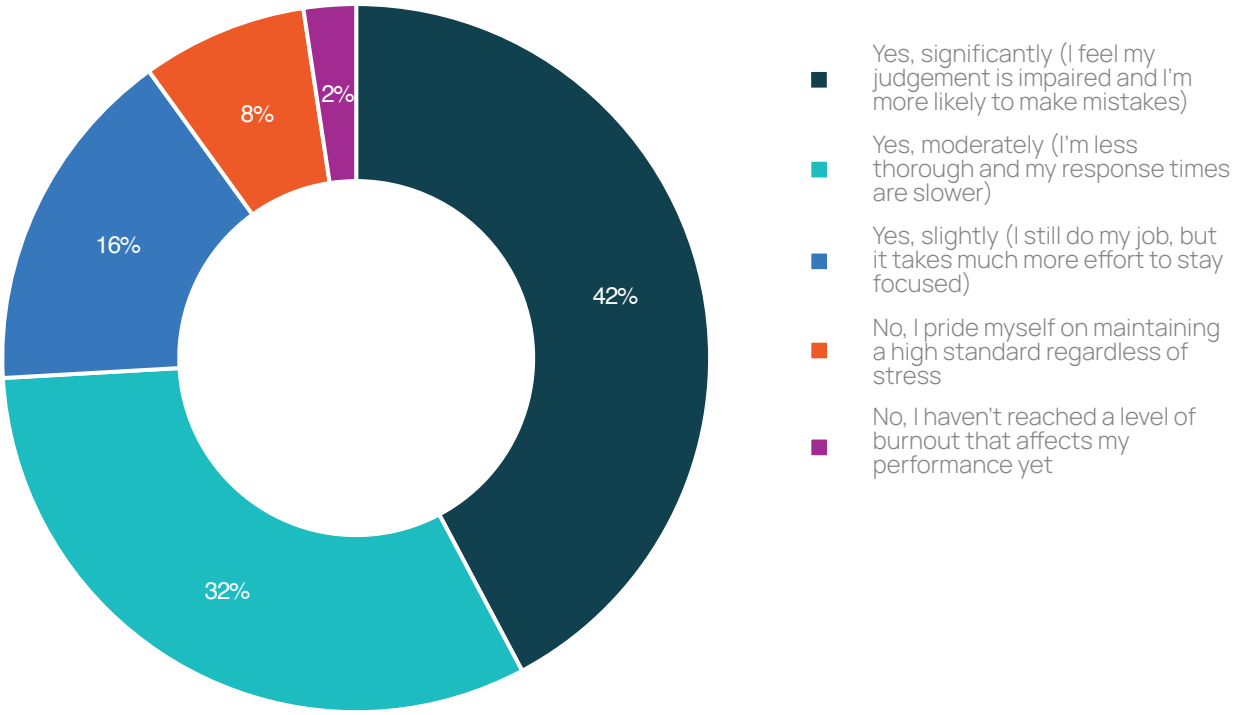
The survey also explored how industry stress impacts the performance of security leaders and, consequently, organisational security. Specifically, we examined how this stress influences their quality of work, attitude, and long-term career plans.

6.1 Quality of work

42% of security leaders say that when they feel overworked, stressed, or burned out, it significantly impairs their ability at work, increasing the likelihood of them making mistakes. Just under a third (32%) said that stress had a moderate impact on the quality of their work.

When security leaders feel stressed and overworked and make mistakes, it's easy to see how a compounding negative spiral could form. Overworked teams make more mistakes, triggering more security incidents and worse outcomes—which ultimately cycles back to pile even more workload and stress onto those same teams.

When feeling overworked, stressed, or burnt out, do you feel like this negatively impacts your ability at work?



06. The impact of stress

6.2 Employee churn

The survey reveals that more than a third of cyber security leaders have taken formal leave from employment due to work stress (37%). A quarter have resigned from a previous role due to stress (26%), and a similar number are currently seriously thinking of doing so (27%).

07. Strategic and operational challenges

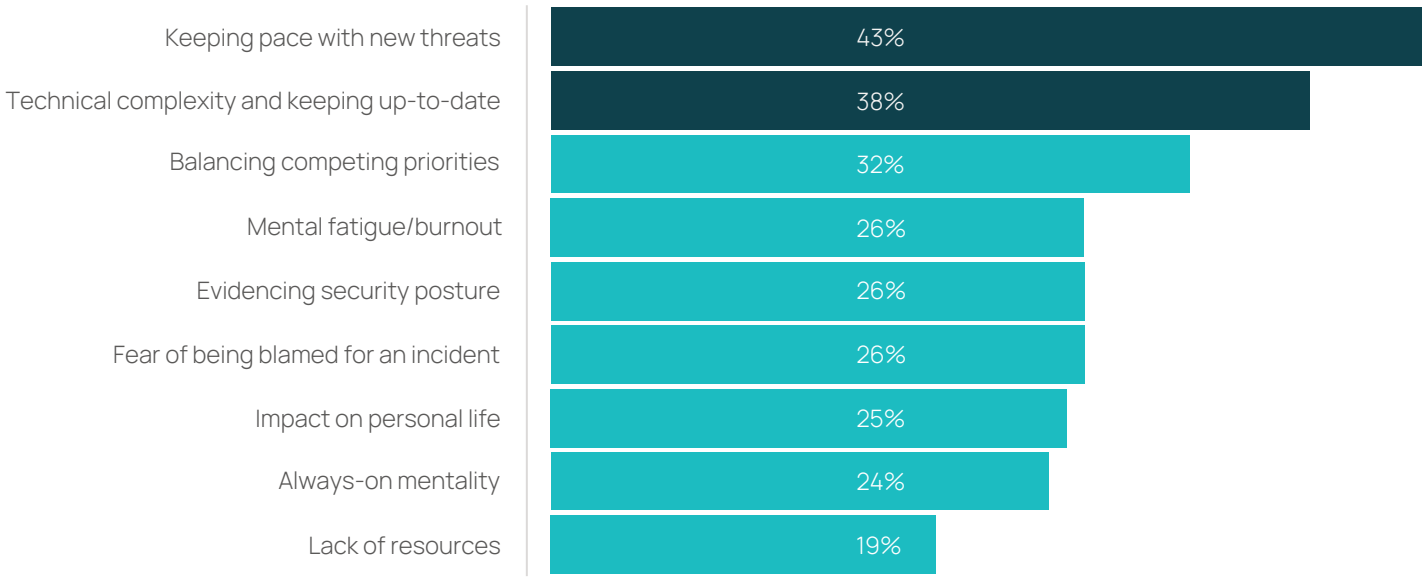
Being a cyber security leader comes with vast and varied demands. Our survey reveals that the two greatest challenges are keeping pace with new threats and navigating technical complexity.

Defending an ever-increasing attack surface requires securing infrastructure, assets, and users against attackers who quickly adapt to exploit both new and legacy vulnerabilities. Give this relentless workload, it is no surprise that security leaders also cite balancing priorities as one of the most difficult aspects of the profession.

Determining where to focus—such as which vulnerabilities to patch or where to improve threat visibility—can be a major headache, especially when shifts in the threat landscape cause priorities to change daily.

Approximately a quarter of cyber security leaders cited mental fatigue and burnout as being among their top challenges. A similar number highlighted the impact on their personal lives, further highlighting the human cost of working in the industry.

What are the most challenging aspects of being a cyber security professional?
(Select 3 answers)



07. Strategic and operational challenges

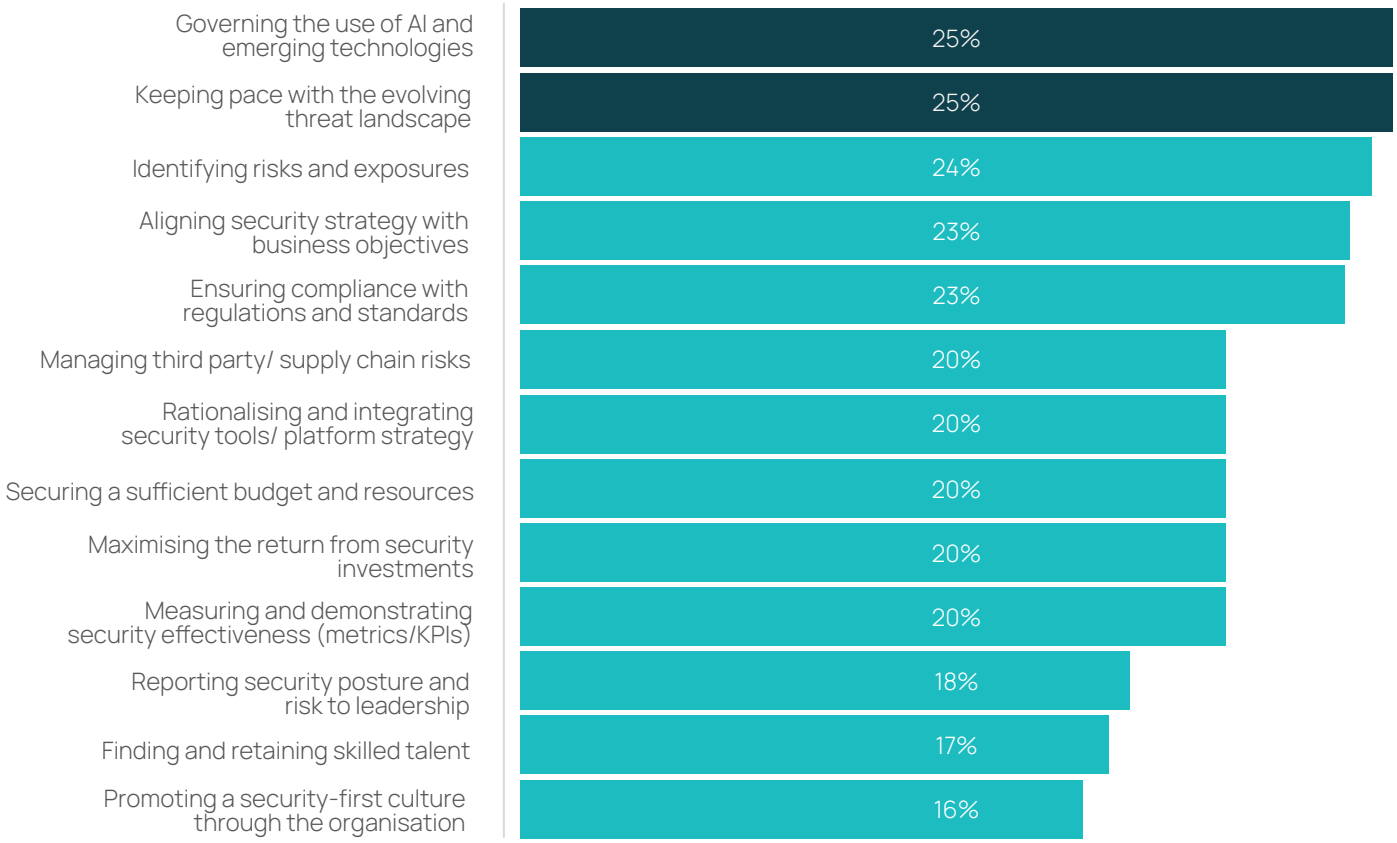
7.1 Strategic challenges

Since 'keeping pace with threats' was selected by security leaders as one of the most challenging aspects of being a security professional, it is no surprise that this same response, along with "identifying risks and exposures," appears in the top three strategic challenges.

Governing the use of AI and emerging technologies' is the challenge cited by the highest number of security leaders (25%). AI is causing widespread disruption, and based on the survey responses, it is clear that many leaders are concerned about how best to utilise this technology in a way that is safe, legal, and generates trustworthy outcomes.

Aligning security strategy with business goals also features highly as a strategic challenge. Because security teams are traditionally viewed as inhibitors of growth, it is encouraging that nearly a quarter of security leaders (23%) identified this as one of their top three strategic challenges.

What are the top three strategic challenges that cause you stress at work?



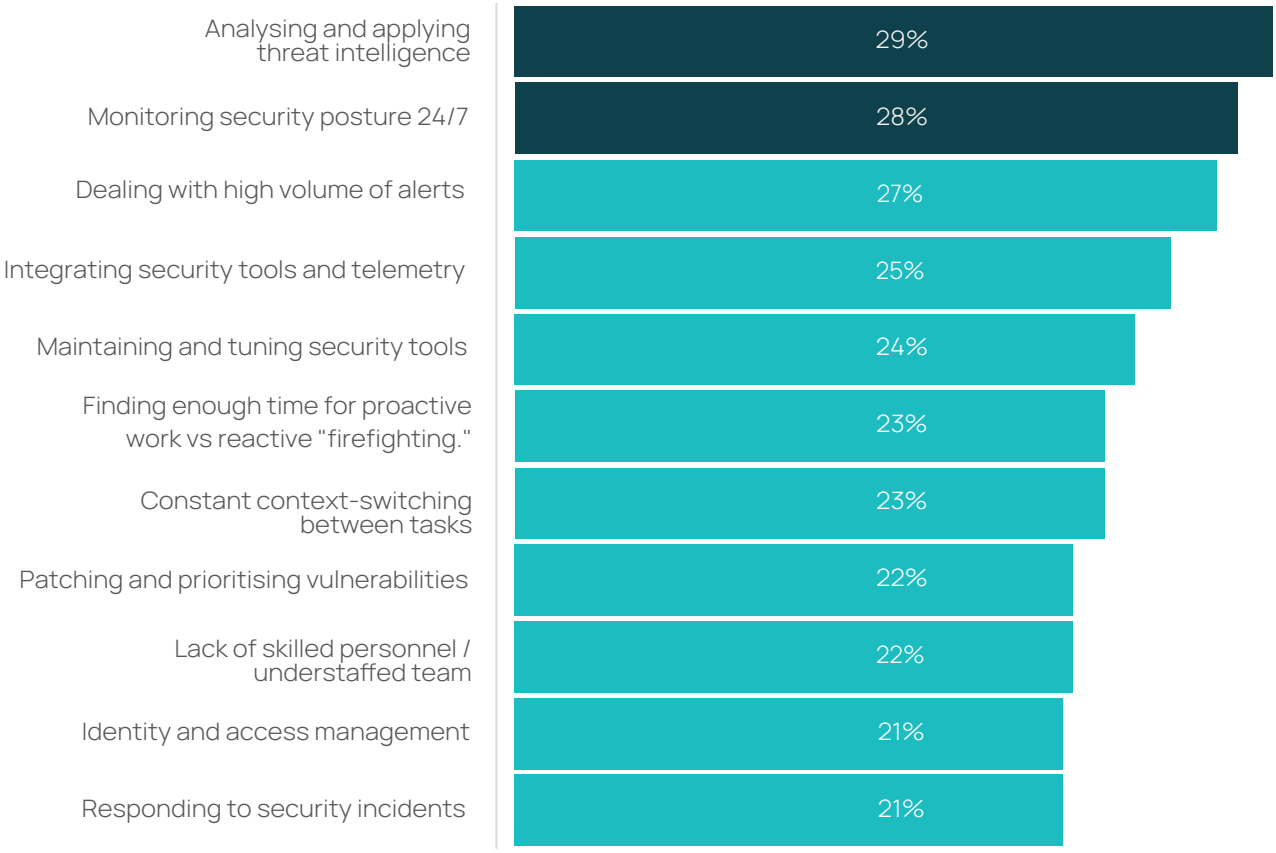
07. Strategic and operational challenges

7.2 Operational challenges

Staying on top of cyber resilience requires an ongoing, around-the-clock commitment to defence. Given this relentless pace, it is understandable that security leaders point to analysing and applying threat intelligence, maintaining 24/7 posture monitoring, and dealing with high volumes of alert volumes as their primary operational stressors.

The complexities of integrating the right security controls—and subsequently maintaining and tuning them to detect and respond to threats—mean that these areas are commonly cited challenges.

What are the top three operational challenges that cause you stress at work?



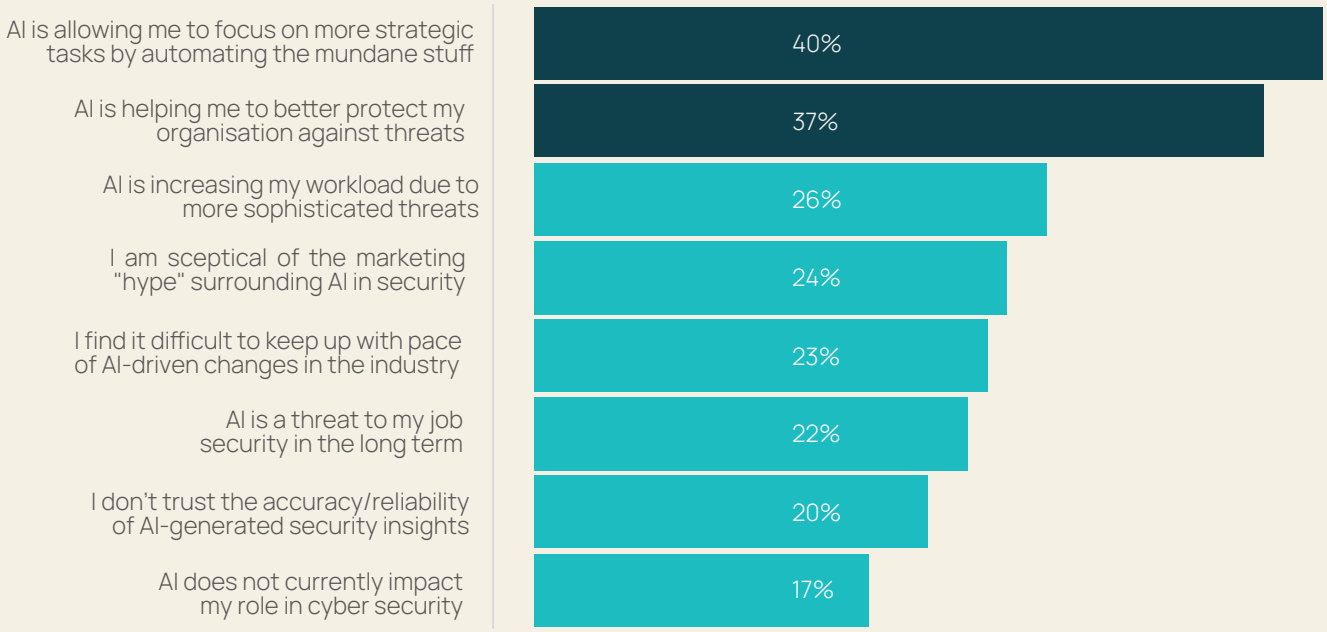
08. The AI challenge and opportunity

Governing the use of AI is one of the most stressful strategic challenges for security leaders. AI is helping cyber security teams work more efficiently and effectively—for instance, enabling SOC teams to accelerate alert triage and analysis. However, in the hands of adversaries, it also has the potential to help them identify and exploit vulnerabilities at scale.

Based on the survey results, it's clear that security leaders have mixed views on AI. While 40% agree that AI allows them to automate routine tasks and focus on more strategic initiatives, a quarter (26%) believe that AI is actually increasing, rather than relieving, their workload.

Twenty-two percent (22%) believe it is a threat to their job in the long term, while 24% are sceptical of the hype, and 20% don't trust its insights.

What are your feelings towards the use of Artificial Intelligence in cyber security?

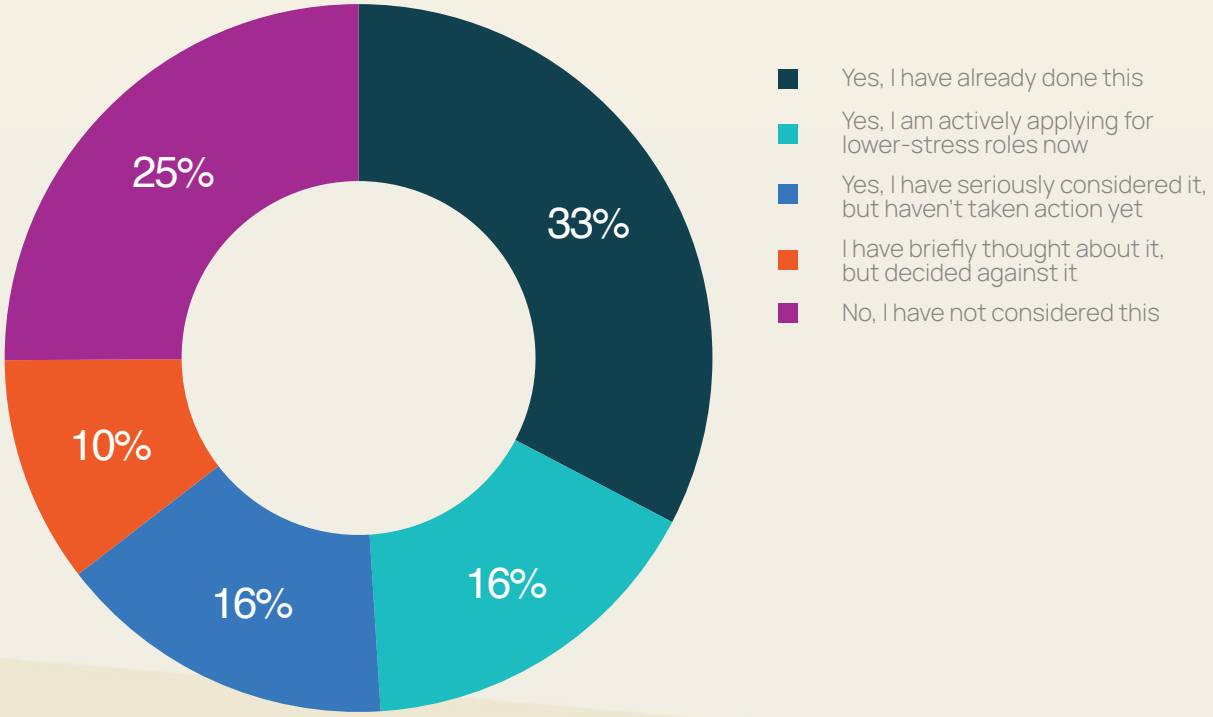


> Nearly a quarter of security leaders believe AI is a threat to their long term job security

09. The pursuit of work-life balance

Cyber security leaders are also choosing to prioritise their mental health over the size of their pay slip. Roughly half (49%) have already taken a pay cut or are actively applying for a lower stress role, or one that offers a better work-life balance.

In the last 12 months, have you seriously considered taking a pay cut in exchange for a role with lower stress or better work-life balance?



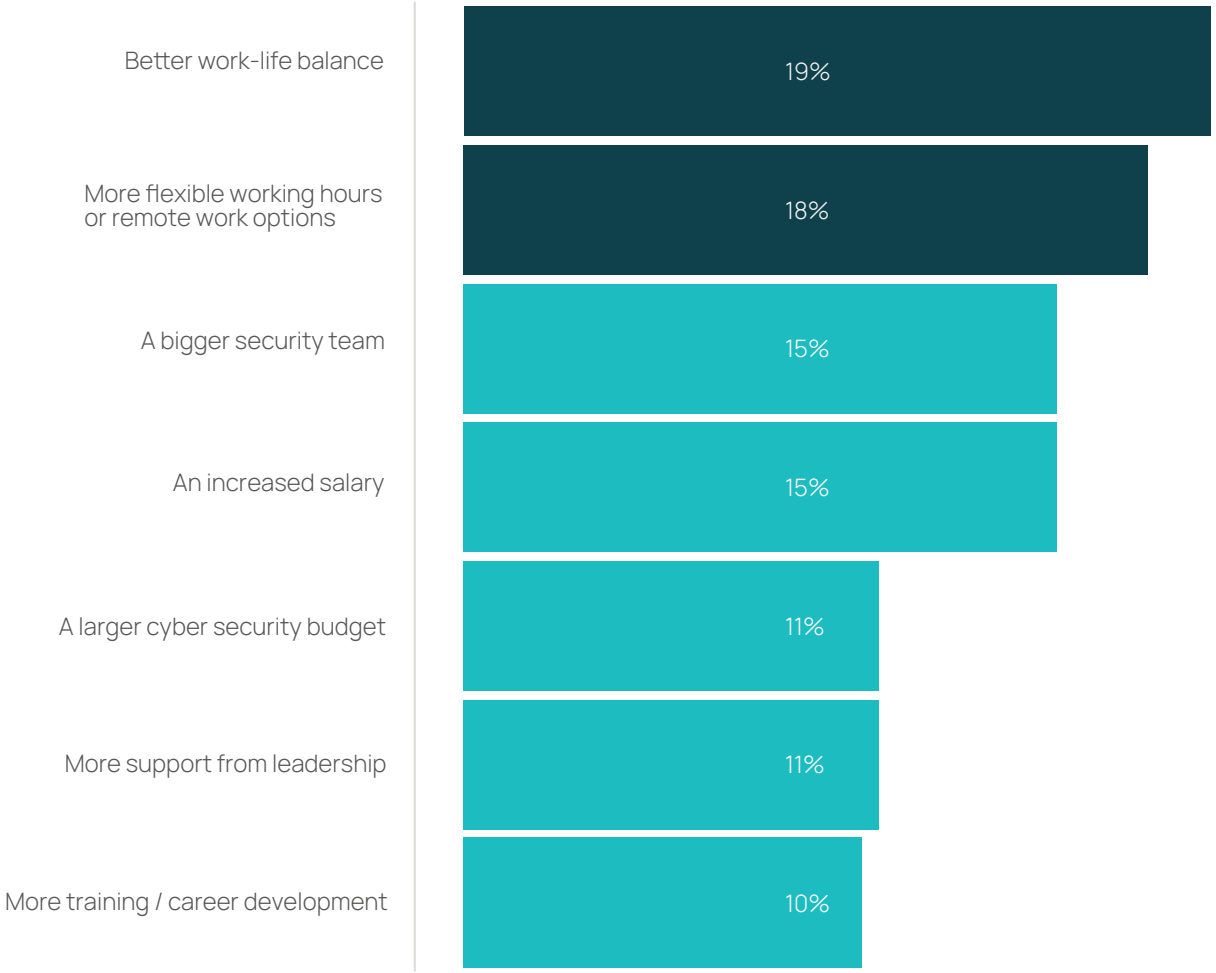
A third of security leaders have taken a pay cut in exchange for a role with less stress or a better work-life balance

09. The pursuit of work-life balance

When security leaders were asked to select the single biggest factor that would improve their enjoyment of the role, the top two responses were a "better work-life balance" and "more flexible hours or remote working options."

Notably, these personal wellbeing factors were more common than operational ones, including a bigger security team, a larger budget, more support from leadership, and additional training. Meanwhile, 15% of security leaders cited higher financial compensation as the primary factor that would improve their enjoyment.

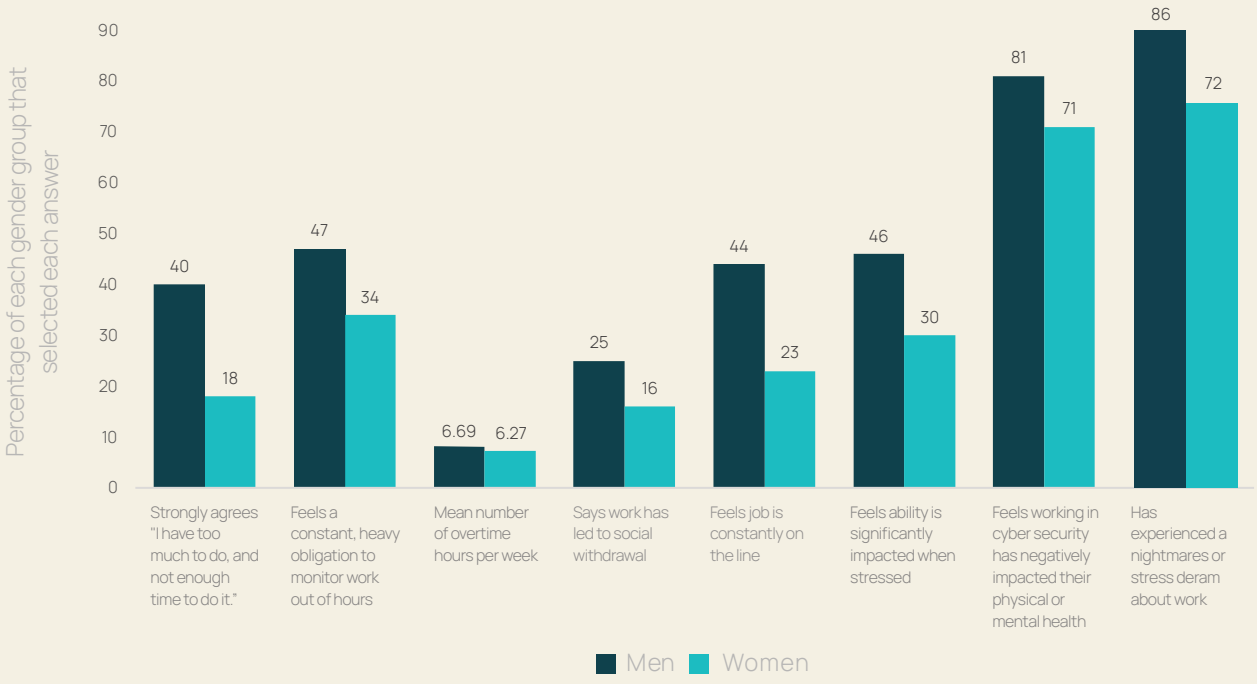
What would be the single biggest factor in helping you to improve enjoyment in your job in cyber security?



10. Stress and wellbeing by gender

Another interesting finding of the survey is the difference in the levels of stress reported by male and female security leaders. Analysing responses relating to work stress, we found that male security leaders consistently reported more negative feelings, behaviours and outcomes compared to female security leaders.

It is not entirely clear why men appear to be more susceptible to work-related stress. Cultural and self-imposed pressures may be a factor. Alternatively, the data may reflect a greater tendency among female security leaders to establish sustainable work-life boundaries and develop better coping mechanisms.



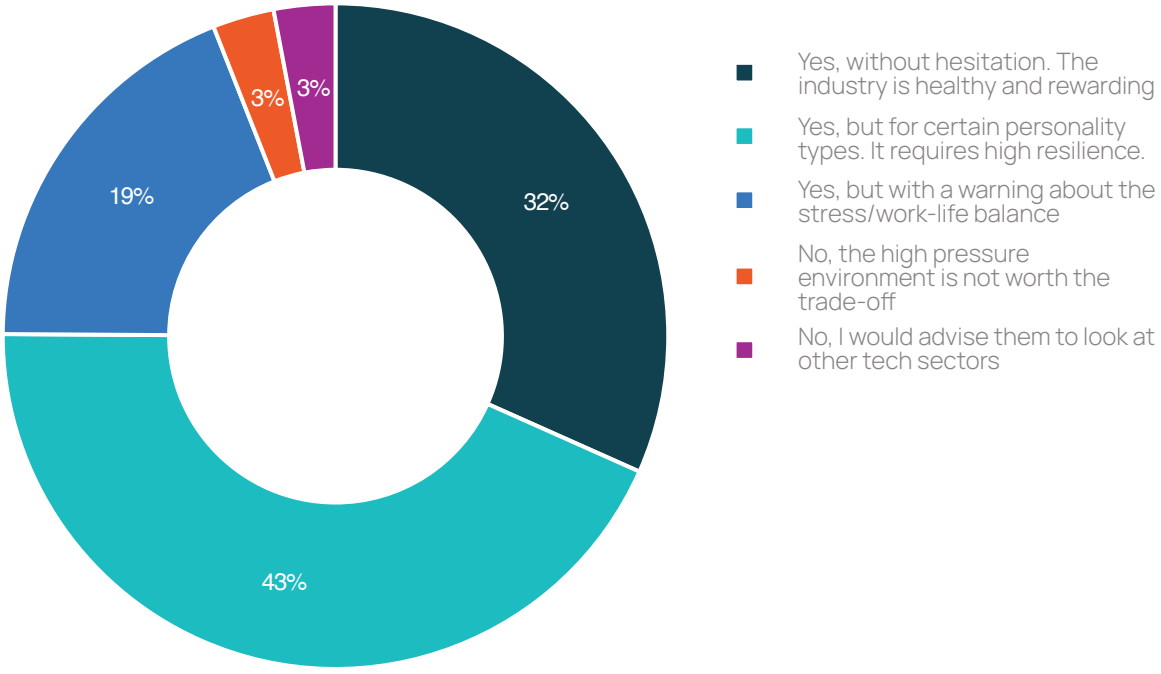
Analysis of survey responses by gender

11. Still a highly recommended career

Despite the stresses and challenges of working in the industry, it's clear that security professionals still view cyber security as an attractive career. Indeed, 94% of cyber security leaders say they would recommend a career in the field.

While 32% recommend a career in cyber security without hesitation, 43% say that they would recommend it for certain personality types only, and 19% would do so with a warning about the stress and impact on work-life balance.

Would you recommend a career in cyber security to a young professional today?



> Despite its challenges, 94% of security leaders would recommend a career in cyber

12. Analysis

Andrew Kays, CEO, Socura

Cyber security has always been challenging, but the burden on leaders in the AI er is heavier than ever.

From the results of our survey, it is clear that security leaders care deeply about their work, drawing a strong sense of pride and fulfilment from protecting their organisations. At the same time, however, they are facing high levels of stress and burnout that are actively impacting their physical and mental wellbeing, and even threatening their long-term future in the industry.

The combination of excessive daily workloads—averaging 38 days of overtime a year—and a pervasive fear of being fired following a security incident is entirely unsustainable. Unless something changes, it is highly likely that we will see more and more professionals quit the industry or transition into lower pressure roles that offer a better work-life balance (as a third of leaders have already done).

The cost of burnout to resilience

In addition to the impact of stress on human wellbeing, the report also highlights a hidden business cost that is less frequently spoken about—the drop in a security leader's productivity and the direct risk this poses to an organisation's resilience. With over 40% of leaders admitting that stress actively impairs their performance, mistakes and poor choices are inevitable—ultimately weakening an organisation's overall defence and response to incidents.

Building sustainable cyber leadership

Supporting security professionals to achieve a healthier work-life balance is key for organisations to ensure the long-term wellbeing of their teams and, ultimately, stronger organisational resilience. This begins by empowering leaders to step back from day-to-day firefighting, granting them the space to focus on high-level strategic initiatives, team development, and critical decision-making. No security leader should be expected to shoulder the full operational burden of maintaining a 24/7 defence.

cont. ▶

12. Analysis

Adoption of AI

The use of artificial intelligence in security operations is creating opportunities for security leaders and their teams to automate routine tasks. However, the challenges of keeping pace with AI-enabled adversaries and safely implementing the technology create their own obstacles. It is revealing that just over half of security leaders feel that AI is actually increasing their workload.

The need for open conversation

While our survey captures the perspectives of leadership, the pressure cooker of cyber security undoubtedly impacts teams at every level. Only by openly discussing the challenges of working in the industry—and sharing strategies to reduce the mental and physical health toll it exacts—can we change the sector for the better and ensure our people can sleep better at night.

> **No security leader should be expected to shoulder the full operational burden of maintaining a 24/7 defence**

13. Industry reaction

Nasser Arif, Cyber Security Manager,
NHS London North West University Trust

As cyber security professionals, we are expertly trained to spot anomalies and vulnerabilities in our tech stacks. But when it comes to our own mental and physical health? We're not nearly as sharp. We can hunt down CVEs all day, yet easily miss the warning signs in our most important asset—ourselves.

The report shows that 78% of us recognise that a career in cyber has negatively impacted our health. And honestly? The real number is probably much higher. Some symptoms , such as a lack of sleep, are common and easy to spot. Others, such as becoming distant or spending less time with loved ones, can be much harder to self-diagnose.

What is clear from the survey is that the symptoms experienced by security leaders will, without a doubt, make individuals less effective in their roles. Those of us in cyber know that this drop in performance could be the exact difference between an attack succeeding or failing at the first hurdle. Threat actors are actively banking on stressed victims missing crucial details.

The difficulty of switching off

It can be incredibly difficult to switch off from the digital world. Personally, I am guilty of constantly checking emails and notifications throughout the workday and during my own time (even when I'm not on call!). It is a bad habit, and one I am actively trying to break. Being reachable 24 hours a day is simply not practical, nor should it be the expected norm.

On a positive note, AI is being embraced as a tool to help cyber professionals automate mundane tasks, allowing them to focus on what really matters. I am hopeful that this will go a long way toward reducing workloads and lowering the barrier to entry for junior talent.

Ultimately, it's great to see that despite the impact on wellbeing, cyber security is still a profession leaders recommend. I personally love this industry and the work I do. Yes, it can be stressful—but with the right support and awareness, the challenges we face are definitely solvable.

13. Industry reaction

Rebecca McKeown, Founder and Principal Psychologist, Mind Science

Socura's 'Sleepless in security' report confirms what many in the industry already know: cyber security is having a profound effect on the wellbeing of its leaders. However, another important trend highlighted by the data is the impact of chronic burnout on judgment and performance right when companies need it most.

The report highlights that the average security leader clocks an extra 38 days of overtime a year, with over 80% feeling a 'very large' or 'large' obligation to be contactable at all times. While the industry loves the myth of a tireless cyber hero, occupational psychology tells a different story—pressure sharpens focus only up to a point. Beyond that, sustained overload causes performance to crater.

Consequently, cyber teams rarely enter crises with a full tank. When such a large number of security leaders admit stress impairs their decision-making, a fatigued lapse during a live breach could mean the difference between containment and catastrophe.

This is worsened by the fact that 86% of leaders dread being fired if a breach occurs. This anxiety shifts the dynamic from real problem-solving to defensive corporate performance; rather than revealing harsh realities, teams naturally shape the story to protect their livelihoods. Under pressure, people compensate by working harder, which hides the toll until it is too late.

Despite the grinding pressure, it's heartening that 94% of security leaders would still recommend a cyber career. This is a profession full of people who care deeply about the work, who find real meaning in it even when it costs them something, and who, given the choice again, would still choose it.

The solution to the problem lies in engaging directly with the cognitive and psychological demands of the role, rather than waiting for symptoms to appear. Just as we train elite athletes or military personnel, we must build cognitive resilience in our cyber teams before the crisis hits.

When an organisation's resilience depends on chronically exhausted teams pulling off miracles, it isn't operating on a strategy—it is relying on luck. And the trouble with luck is that it always runs out eventually.

About Socura

Socura is a Managed Detection and Response provider bringing the power of calm to organisations across the UK. In an ever-changing landscape, we empower teams with the clarity, control, and confidence to minimise cyber security risk and thrive.

Trusted by businesses and critical infrastructure, we deliver a precise, measured, and personal service that shuts down threats swiftly and effectively. We're proud to be ranked among the top 100 managed security service providers globally.

socura.co.uk

15. Appendix

Copy of the survey

Q1. Which of the following best describes your personal perspective on the 'high-stakes' nature of a career in cyber security? ‹Single code›

- High-stakes and highly motivating: I enjoy the importance and "mission-critical" nature of the work
- High-stakes and highly stressful: The weight of the responsibility is a major source of anxiety
- High-stakes but balanced: I recognise the importance but have the tools/support to manage it
- Artificially high-stakes: The "stakes" are often exaggerated
- Standard-stakes: It is no more critical than IT or infrastructure roles
- None of the above statements

Q2. What are the most challenging aspects of being a cyber security professional? ‹Multi code Top 3›

- Always-on mentality
- Keeping pace with new threats
- Balancing competing priorities
- Technical complexity and keeping up-to-date
- Mental fatigue/burnout
- Impact on personal life
- Fear of being blamed for an incident
- Evidencing security posture
- Lack of resources
- Other (please specify)

15. Appendix

Q3. How much do you agree: "I have too much to do, and not enough time to do it?" ‹Single code›

- Strongly agree
- Agree
- Neutral / Undecided
- Disagree
- Strongly disagree

Q4. To what extent do you feel obliged to monitor work communications or alerts outside of your contracted hours? ‹Single code›

- To a very large extent – I feel a constant, heavy obligation to be reachable at all times
- To a large extent – I feel a significant duty to be available and monitor updates
- To a moderate extent – I feel I should stay updated, but it doesn't dominate my time
- To a small extent – I check occasionally, but don't feel "required" to
- Not at all – I feel zero obligation to check work after hours

Q5. On average, in the last 12 months, how often have you been called out/alerted after hours due to a cyber incident? ‹Single code›

- Once a week or more (Chronic/High-intensity)
- 2–3 times per month (Frequent)
- 7–12 times per year (Roughly once a month)
- 3–6 times per year (Bimonthly)
- 1–2 times per year (Rare/Exceptional)
- Never

15. Appendix

Q6. On average, how many overtime hours do you work per week (paid or unpaid)?
‹Slider›

- 0 hours
- Less than 5 hours (Occasional late nights)
- 6–10 hours (Equivalent to one extra workday per week)
- 11–15 hours (Working most evenings/weekends)
- 16+ hours (Two or more extra workdays per week)

Q7. What are the top three strategic challenges that cause you stress at work?
‹Multi code›

- Keeping pace with the evolving threat landscape
- Identifying risks and exposures
- Managing third party/ supply chain risks
- Governing the use of AI and emerging technologies
- Securing a sufficient budget and resources
- Promoting a security-first culture through the organisation
- Finding and retaining skilled talent
- Reporting security posture and risk to leadership
- Maximising the return from security investments
- Aligning security strategy with business objectives
- Rationalising and integrating security tools / platform strategy
- Measuring and demonstrating security effectiveness (metrics/KPIs)
- Ensuring compliance with regulations and standards

15. Appendix

Q8. What are the top three operational challenges that cause you stress at work? Multi choice ‹Multi code›

- Monitoring security posture 24/7
- Dealing with high volume of alerts
- Responding to security incidents
- Patching and prioritising vulnerabilities
- Monitoring and applying threat intelligence
- Maintaining and tuning security tools
- Integrating security tools and telemetry
- Identity and access management
- Finding enough time for proactive work vs. reactive "firefighting."
- Constant context-switching between tasks
- Lack of skilled personnel / understaffed team
- Other (please specify)
- None of the above

Q9. Do you worry that you might get fired if there is a serious security incident at your workplace? ‹Single code›

- Always – I feel my job is constantly on the line
- Often – I worry about this during any major alert
- Sometimes – It crosses my mind during significant incidents
- Rarely – I feel relatively secure in my position
- Never – I trust my organisation's "no-blame" culture

15. Appendix

Q10. When feeling overworked, stressed, or burnt out, do you feel like this negatively impacts your ability at work? ‹Single code›

- Yes, significantly (I feel my judgement is impaired and I'm more likely to make mistakes)
- Yes, moderately (I'm less thorough and my response times are slower)
- Yes, slightly (I still do my job, but it takes much more effort to stay focused)
- No, I pride myself on maintaining a high standard regardless of stress
- No, I haven't reached a level of burnout that affects my performance yet

Q11. What are your feelings towards the use of Artificial Intelligence in cyber security? ‹Multi code›

- AI is increasing my workload due to more sophisticated threats
- I find it difficult to keep up with the pace of AI-driven changes in the industry
- AI is helping me to better protect my organisation against threats
- I don't trust the accuracy/reliability of AI-generated security insights
- AI is allowing me to focus on more strategic tasks by automating the mundane stuff
- AI is a threat to my job security in the long term
- I am sceptical of the marketing "hype" surrounding AI in security
- AI does not currently impact my role in cyber security
- None

15. Appendix

Q12. Do you believe working in cyber security has ever negatively impacted your physical and mental health ‹Single code›

- Physical health
- Mental health
- Both
- None
- Prefer not to say

Q13. n the last 12 months, have you experienced any of the following due to work? ‹Multi code›

- Lack of sleep / Insomnia
- Nightmares/bad dreams about work
- Anxiety or panic attacks
- Physical symptoms (e.g., high blood pressure, headaches, digestive issues)
- Changes in eating habits or weight
- Irritability or low patience with others
- Depression
- Social withdrawal (avoiding family, friends, or hobbies)
- Feelings of burnout or emotional exhaustion
- Difficulty concentrating or "brain fog"
- Increased use of substances (e.g., alcohol, caffeine, nicotine) to cope
- None of the above

15. Appendix

Q14. In the last 12 months, have you experienced a nightmare or stress dream about a cyber incident at work? ‹Single code›

- Yes, I have recurring stress dreams about work
- Yes, frequently (monthly or more)
- Yes, occasionally (every few months)
- Yes, once or twice
- No, never

Q15. Have you ever taken formal leave, resigned, or seriously considered resigning due to work stress? ‹Multi code›

- I have taken formal leave (sick leave/mental health leave) due to work stress
- I have resigned from a previous role due to work stress/burnout
- I have thought about resigning due to work stress
- I am currently seriously considering resigning due to workplace stress
- No, I have never reached this point

Q16. In the last 12 months, have you seriously considered taking a pay cut in exchange for a role with lower stress or better work-life balance? ‹Single code›

- Yes, I have already done this
- Yes, I am actively applying for lower-stress roles now
- Yes, I have seriously considered it, but haven't taken action yet
- I have briefly thought about it, but decided against it
- No, I have not considered this

15. Appendix

Q17. What would the single biggest factor in helping you to improve enjoyment in your job in cyber security? ‹Single code›

- A bigger security team
- An increased salary
- A larger cyber security budget
- More support from leadership
- More training / career development
- Better work-life balance
- More flexible working hours or remote work options
- Other (please specify)

Q18. Would you recommend a career in cyber security to a young professional today? ‹Single code›

- Yes, without hesitation. (The industry is healthy and rewarding)
- Yes, but only for certain personality types. (It requires high resilience)
- Yes, but with a warning about the stress/work-life balance
- No, the high-pressure environment is not worth the trade-off
- No, I would advise them to look at other tech sectors

socura.co.uk