2024

HACKTHEBOX

Building a firewall against cybersecurity burnout

Table of contents

03 Protecting a business starts with protecting its people

04 Report methodology

05 Key takeaways

06 The burnout landscape. Spreading like wildfire.

10 The financial cost to businesses

11 The burnout gap

16 The enterprise approach to battling burnout

18 Connecting cyber with the board

19 Support for CISOs

20 Building a firewall against burnout

23 Proactive steps forward

24 About Hack The Box

Protecting a business starts with protecting its people

HARIS PYLARINOS
Founder & CEO
@ Hack The Box

Since the start of the pandemic, cybercrime has surged by nearly 600%. 84% of cybersecurity professionals are experiencing burnout, which is directly affecting performance.[1] With human error as the cause of most incidents and breaches, mental health in the industry should be addressed as the first concern of technical leaders. To prepare for cyber breaches, companies must prioritize providing their workforce with the support necessary to bring out the best version of themselves, day in and day out.

Our research shows that burnout isn't just taking a toll on cybersecurity professionals but the businesses themselves. Those working in cybersecurity and infosecurity roles at medium to large enterprises surveyed say that work-related poor mental well-being is making them less productive and taking sick leave due to stress, fatigue, or burnout - costing medium to large enterprises across the UK over £130 million and across the US over $626 million per year in lost productivity. 74% of business leaders say that cybersecurity and infosecurity teams have taken time off due to stress, fatigue, or burnout, leaving businesses at higher risk of breaches with a weakened workforce.

Hack The Box is on a mission to create and maintain high-performing cybersecurity individuals and organizations. This means helping security leaders across the globe to equip their teams with the skills and expertise they need to proactively secure and protect their organization, as well as designing career development programs to further help prevent employee burnout and enhance talent retention. This takes a commitment from the businesses too, but also from the industry to explore the true cause and solutions to stress, fatigue, or burnout and build effective strategies for change.

Protecting an organization has always been the priority but this means not just defending against threats but protecting the cybersecurity professionals so they can defend the organization. Without cyber professionals being able to deliver their jobs efficiently, grow skills faster and better, and cultivate a healthier work environment through continued support, and mental and physical resilience, businesses will always be at a higher risk. Businesses need to build a firewall around their professionals. Once they are protected, they will protect the businesses.

[1] How to Combat Cybersecurity Burnout — and Keep Your Company Secure, Mimecast

Report methodology

Hack The Box commissioned an independent market research company, Censuswide, to survey two samples.

The first sample was 1,001 full-time enterprise business leaders specialized in cybersecurity and infosecurity in medium and large enterprises between May 20, 2024, and May 24, 2024. The second sample was 1,207 full-time cybersecurity & infosecurity professionals within medium and large enterprises in the UK and US between May 20, 2024, and May 24, 2024. Censuswide abides by and employs members of the Market Research Society and follows the MRS code of conduct and ESOMAR principles. Censuswide is also a member of the British Polling Council.

Unless stated otherwise, all figures were drawn from this poll.

Key takeaways

UK
£130 million

US
$626 million

On average, medium to large enterprises are losing over **£130 million** annually in the UK and over **$626 million** in the US due to lost productivity coming from stress, fatigue, or burnout.

UK
41%
£3-4 million

US
45%
$2.5-3.8 million

41% of business leaders in the UK and **45%** in the US estimate the 12-month financial cost of stress, fatigue, or burnout for their businesses to be **£3-4 million** and **$2.5-3.8 million,** respectively.

90% of CISOs are concerned about stress, fatigue, or burnout affecting their team's well-being.

74% of business leaders report staff taking time off due to stress, fatigue, or burnout.

53% of business leaders confirm they do not outsource upskilling platforms and providers to ensure the latest training and tools, crucial for enhancing cyber resilience and employee well-being.

51% of business leaders admit they do not provide transparent and competitive career development programs for their cybersecurity and infosecurity teams.

59% of business leaders confirm they do not invest in new tools to enable teams to do their roles more effectively.

45% of business leaders reveal they increase wages to improve employee satisfaction rather than addressing the root cause of burnout.

65% of cybersecurity and infosecurity professionals have experienced stress, fatigue, or burnout due to skill gaps and pressure to perform beyond their capabilities.

8% of cybersecurity and IT professionals say they are considering quitting their jobs due to overtime, stress, burnout, or mental health challenges within their role in cybersecurity.

The burnout landscape. Spreading like wildfire.

The threat landscape is constantly evolving with increased breach attempts, new technologies, and techniques employed by threat actors such as AI, and increasing numbers of criminal groups. Businesses are finding that cybersecurity professionals are working beyond their contracted hours. 66% of business leaders say that the top reasons why cybersecurity and infosecurity professionals are working over their contracted hours are due to increased numbers of cybersecurity threats and unpredictable threats after work hours.

74% of business leaders also report that cybersecurity and infosecurity professionals take time off due to stress, fatigue, or burnout.

According to Statista cyber-attacks were most prevalent in manufacturing **(26%)** as well as in finance and insurance **(18%)** industries. These industries also see employees taking more sick leaves due to mental health issues, as indicated by the research:

86%
IT & Telecoms

81%
Finance

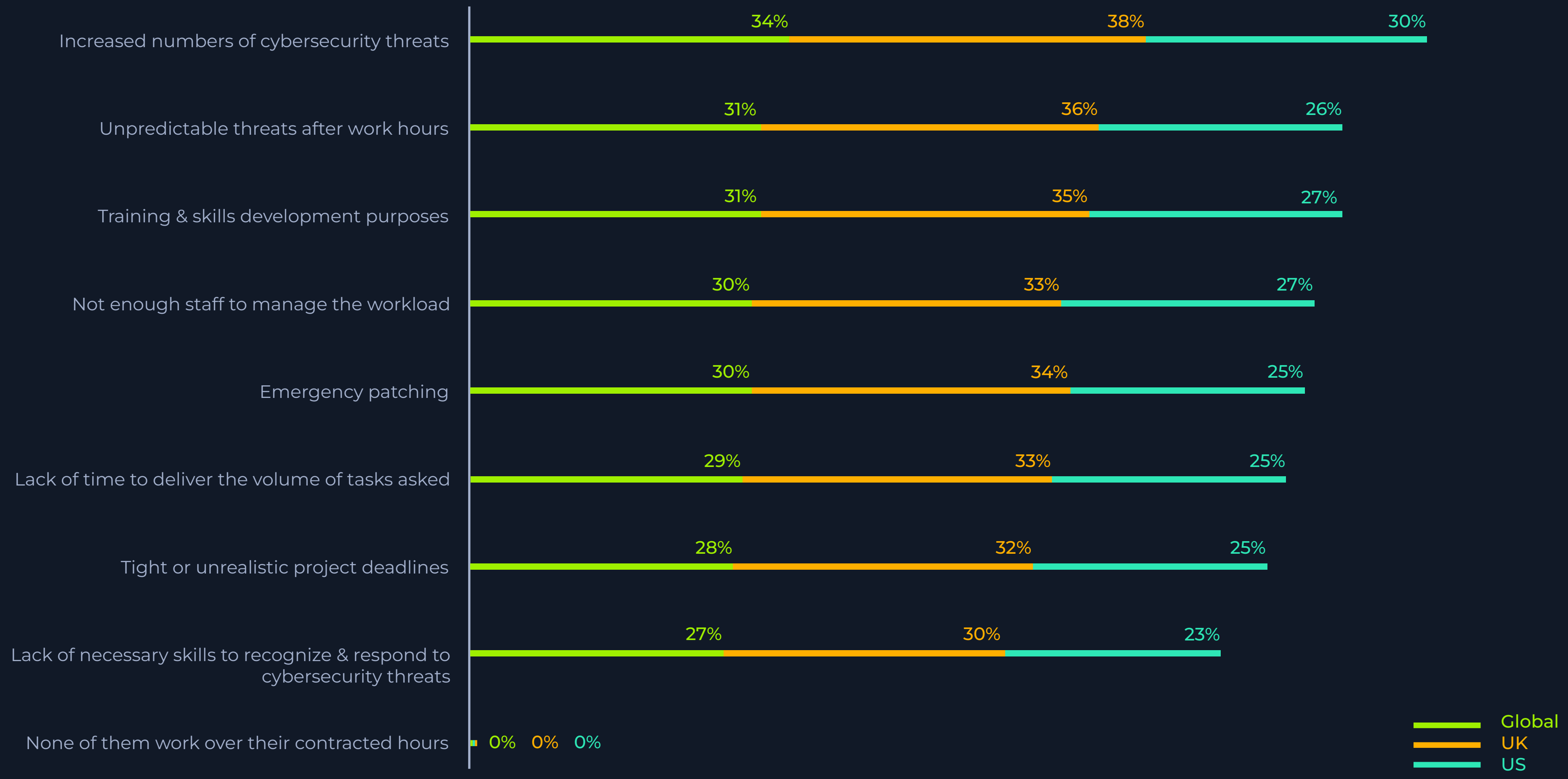
78%
Manufacturing & Utilities

75%
Healthcare

This is leaving teams understaffed and under-resourced, leading to reduced talent retention, increased risk of errors, and reduced time or appetite for upskilling. On top of that, a lot of professionals are considering exiting the industry, further exacerbating the skills shortage.

The burnout landscape. Spreading like wildfire.

Fig. 1: **Business leaders'** reasons why cybersecurity and infosecurity professionals work over their contracted hours



The burnout landscape. Spreading like wildfire.

Contrary to the perspective of business leaders, cybersecurity and infosecurity professionals see the cause of burnout as a skills and workload issue. Overall, **89%** of professionals say the workload, volume of projects to deliver, and the time needed to deliver tasks are the key causes of burnout. In addition, they are experiencing pressure to perform outside skillset, which ranks as a second key cause of burnout with **66%**.

This indicates the **need for more mutual understanding** between cybersecurity teams and business leaders about what is causing stress, fatigue, or burnout.

Fig. 2: **Cybersecurity and infosecurity professionals** felt stress, fatigue, or burnout due to work for the following reasons

Reason for burnout	Overall	UK	US
Lack of skills within the wider team	24%	26%	22%
Lack of time to deliver the tasks asked	23%	26%	19%
High workload	23%	24%	21%
Overwhelmed due to the high volume of cyber incidents	23%	25%	21%
High volume of projects and tasks to deliver	22%	23%	22%
Incorrect hiring expectations	22%	20%	24%
Pressure to perform outside of skillset	22%	20%	23%
Lack of talent and resources within the team	21%	23%	18%
Lack of a clear career path	21%	20%	21%
Lack of skills to deliver results	20%	21%	19%

> Burnout is particularly prevalent in the cybersecurity industry due to the high stakes and constant pressure professionals face. Cybersecurity teams often deal with a high volume of threats, tight deadlines, and the ever-present knowledge that a single oversight could lead to significant breaches. The “always-on” nature of the job, coupled with a global shortage of skilled cybersecurity professionals, means many are working long hours under intense scrutiny. This relentless pace without sufficient downtime can lead to burnout.

Andrea Succi, CISO at Ferrari Group

FERRARI

The financial cost to businesses

Stress, fatigue, or burnout throughout a workforce can have a significant financial cost to businesses. Business leaders across medium and large enterprises have predicted that burnout costs them **just under £3 million in the UK** and **over $3 million in the US.**

The cost to productivity according to our research is £130 million in the UK and $626 million in the US. The average number of sick days taken each year per worker is **3.4** and the average number of days lost due to poor productivity is estimated as **3.4 hours** per month, per worker. This is an additional 5.1 days per year (assuming an 8-hour working day) which equals **8.5 days per year per worker lost to poor mental health.** There is a serious cost issue without even considering the human impact on individuals.

Fig. 3: Business leaders in the UK and the US estimate the financial cost of burnout for their business within a 12-month period including, the cost of replacement staff, recruitment fees, paid overtime, and any other associated expenses

	4%	15%	30%	41%	11%
Estimated cost of burnout	Up to £1 million	Over £1 million, up to £2 million	Over £2 million, up to £3 million	Over £3 million, up to £4 million	Over £4 million, up to £5 million

UK business leaders of medium to large enterprises

	3%	13%	45%	31%	8%
Estimated cost of burnout	Up to $1.3 million	Over $1.3 million, up to $2.5 million	Over $2.5 million, up to $3.8 million	Over $3.8 million, up to $5 million	Over $5 million, up to $6.3 million

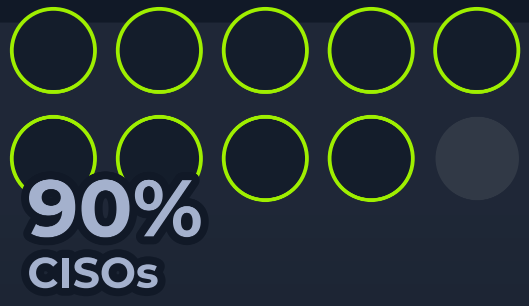
US business leaders of medium to large enterprises

The burnout gap

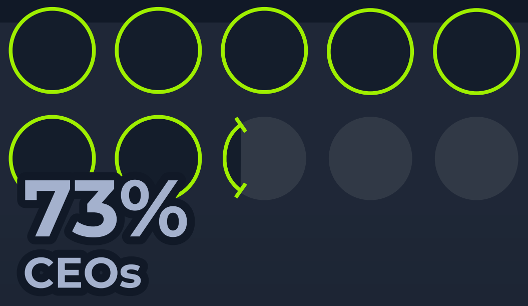
We have already seen that the causes of burnout reported by cybersecurity and infosecurity professionals are different from those listed by business leaders, indicating a gap between the two groups. The consequences of burnout also show the different perceptions between professionals, CISOs, and CEOs.

Business leaders are indeed concerned about burnout resulting in poor staff mental well-being and an unengaged workforce. However, they are least concerned about professionals exiting the industry even though there is still a significant recruitment shortage.

It is worth highlighting the significant differences between the different board members.



90% of CISOs are concerned about cybersecurity and infosecurity staff stress, fatigue, or burnout impacting their well-being.

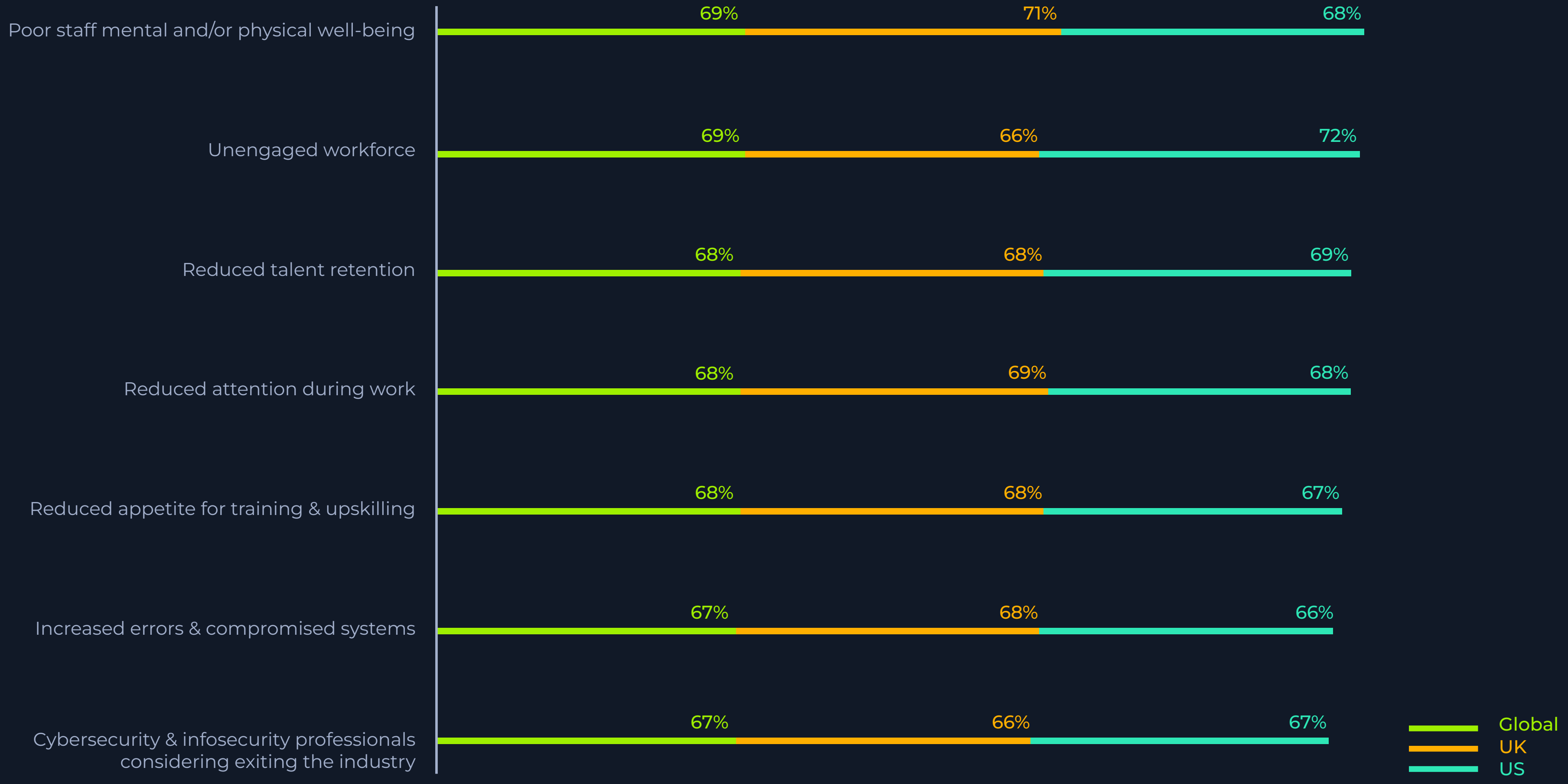


In contrast, only **73% of CEOs** are concerned about the impact of cybersecurity staff stress, fatigue, or burnout on both well-being and errors, with **47%** highlighting the latter.

CISOs are deeply connected to the cybersecurity industry, staying attuned to its trends, impacts, and the challenges that cybersecurity and infosecurity professionals face. Additionally, CISOs are experiencing their own pressure to perform and are increasingly affected by burnout. On the other hand, **CEOs** often appear less concerned about the well-being of their cybersecurity teams, primarily because they are less connected to the realities of the team's roles and experiences.

The burnout gap

Fig. 4: Business leaders' concerns on the impact of cybersecurity and infosecurity staff stress, fatigue, or burnout



The burnout gap

The perspective of cybersecurity professionals seems quite different as they are working serious additional overtime impacting their mental well-being and personal lives, adding to stress and fatigue. **68%** of cybersecurity and infosecurity professionals work between **10 and 50 hours** of unpaid overtime hours per week. **76%** have taken between **3 and 6 sick days** over the past year due to work-related well-being problems. In addition, **35%** have not used **3 to 5 days** of annual leave in the last 12 months due to heavy workloads.

Professionals are listing various reasons as the impact of stress, fatigue, or burnout. One of the highest-rated impacts are on missing key milestones for their children, which has repercussions on their personal lives and relationships, as well as **feeling that hiring expectations were not consistent with the job role,** and **concerns over not meeting senior expectations.** This additional stress of delivering on workload matched with inconsistent job expectations impacts motivation, job satisfaction, and ultimately retention. Although business leaders are least concerned about professionals exiting the workforce, **8%** of respondents are considering exiting the cybersecurity industry. With a current and serious skills shortage, this is not to be disregarded.

12% of cybersecurity and infosecurity professionals missing key personal milestones may seem like a low figure, but this is a significant portion of the workforce. That is 12% of every team and thousands of cybersecurity professionals.

ISC2 – the world's leading nonprofit member organization for cybersecurity professionals – estimates the global cybersecurity workforce has reached 5.5 million people. This means 660,000 cybersecurity and infosecurity professionals have missed a key personal milestone, such as their child's birthday.

Fig. 5: The direct impact of stress, burnout, or mental health challenges on cybersecurity and infosecurity professionals due to their role

Impact	Overall	UK	US
Decreased performance in non-work-related tasks (e.g., household chores, volunteer work)	13%	13%	12%
Missed a milestone for children (e.g., child's birthday or school commitment)	12%	12%	11%
Feeling like initial hiring expectations were not consistent with the actual job requirements	12%	13%	12%
Feeling like I am not meeting senior team expectations due to being unable to deliver the workload expected	12%	12%	11%
Feeling like my boss didn't understand what I do	12%	13%	10%
Feeling unsupported by my organization regarding tools to support my health and well-being	11%	14%	8%
Feeling like I would benefit from mental health/well-being support external to the company	11%	14%	8%
Neglected self-care activities (e.g., exercise, relaxation, hobbies, leisure activities)	11%	11%	10%
Feeling like I would benefit from mental health/well-being support within the company	11%	11%	10%
Missed deadlines for personal projects or commitments	11%	11%	10%
Had to cancel plans with friends and family	10%	10%	11%
Decreased job satisfaction or motivation	10%	12%	8%
Lack of time to train and upskill within cybersecurity	10%	11%	9%
Feeling like my company didn't offer enough mental health support	10%	10%	10%
Increased stress or anxiety leading to physical health issues	10%	9%	10%
Feeling like my cybersecurity skills were not up to scratch	10%	11%	9%
Delayed career progression	10%	10%	9%
Considering a new job but within cybersecurity/Infosecurity	9%	11%	8%
Feeling like I was not part of the company's goals or priorities	9%	9%	10%
Feeling like I am not upskilled to do my job	9%	10%	9%
Had to work on a bank holiday, Christmas, or over a holiday period	9%	9%	9%
Had to cancel a holiday	9%	8%	9%
Overwork has had a knock-on impact on my personal relationships	8%	8%	9%
Had to cancel my annual leave	8%	8%	9%
Considering a new career outside of cybersecurity	8%	8%	8%
Quit my job	8%	7%	9%

> The cybersecurity domain is a very stressful career to pursue, requiring strong decision-making skills in various aspects. Additionally, mistakes in this field can be catastrophic, especially considering the 24/7 on-call responsibilities throughout the year. High workload, pressure, continuous on-call duties, high stakes, and accountability are a few causes of burnout.

Husam Shbib, Information Security Consultant at TrustLink

The enterprise approach to battling burnout

It is clear that proactive solutions are needed to mitigate stress, fatigue, or burnout. The majority of businesses are not taking action to improve employee well-being, thereby failing to prevent these kinds of challenges.

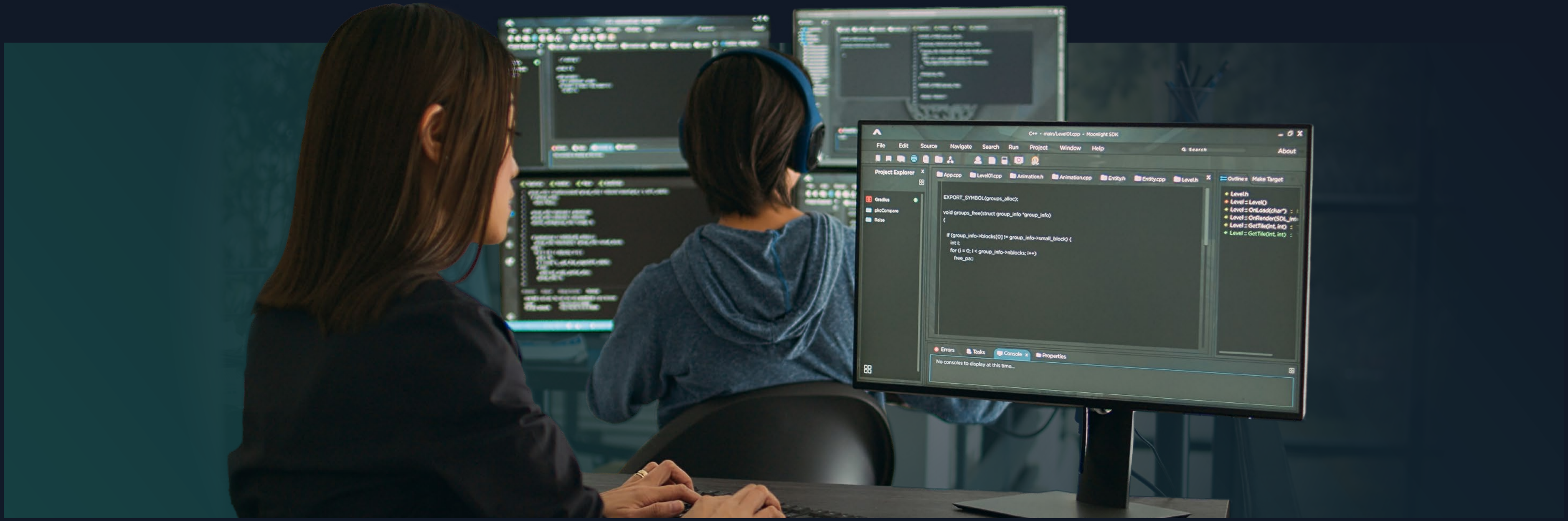
On average **53%** of businesses do not invest in the latest training and tools to ensure their staff performs effectively and **51%** do not provide transparent and competitive career development programs. Proactive action is not being taken across the industry to mitigate this significant issue.

Fig. 6: Actions not taken by business leaders to improve cyber resilience and employee well-being to prevent stress, fatigue, or burnout[2]

Action	Overall	UK	US
Do not provide transparent and competitive career development programs	51%	52%	50%
Do not outsource upskilling platforms and providers to ensure employees have the latest training and tools to deliver against their roles	53%	59%	47%
Do not provide access to mental health support tools: inc. counselors, therapists, or trained professionals	54%	59%	50%
Do not invest in internally upskilling and training team members to deliver against their roles	56%	62%	49%
Do not ensure the cybersecurity lead was given up-to-date cyber upskilling	55%	57%	54%
Do not increase wages	55%	58%	53%
Do not invest in additional temporary staff when teams are stretched to avoid burnout and stress	56%	60%	52%
Do not invite the cybersecurity lead to head of department meetings	56%	59%	53%
Do not regularly complete staff surveys to find out the true cause of stress and burnout	58%	61%	55%
Do not hire temporary staff for under 6 months	59%	63%	55%
Do not provide time off in place of any time worked outside of contracted hours	59%	61%	56%

[2] Responses in figure 6 relate to 1001 full-time enterprise business leaders specialized in cybersecurity and infosecurity in medium and large enterprises and their responses on what they do to manage Cybersecurity and Infosecurity workforce, including improving cyber resilience and employee well-being and demonstrating those that didn't selection these options.

The enterprise approach to battling burnout



Business leaders need to prioritize the right actions to get support to their cybersecurity and infosecurity teams. Inviting cybersecurity leads to head-of-department meetings and completing staff surveys to find out the true cause of stress, fatigue, or burnout are not going far enough. However, more organizations are investing in outsourcing upskilling to ensure employees feel they have the skills to do a successful job, which is essential and a positive move in the right direction.

In addition, providing transparent and competitive career development programs ensures that employees are seen as a long-term part of the company, are valued and that they have a clear way through to progress. More organizations do need to provide access to mental health support tools such as counselors, therapists, or trained professionals, not just to recognize burnout but to reduce and improve that from the very beginning.

Connecting cyber with the board

Listening to what cybersecurity and infosecurity professionals need to prevent burnout means a revamp and assessment of how global operations work within large organizations. Considering how teams are structured, how they communicate and the responsibilities between team members needs to be clear. Working overtime due to global operations means that overtime is systematically happening without the additional expectations of threats outside of work hours.

In addition, staffing levels need to be considered seriously. This means additional team members, either temporary or permanent. However, when hiring for these roles, a clear assessment of the skills needed for the role needs to be undertaken and then ensuring that the recruitment process sources talent that has the skills for the role advertised. If roles are filled but the skills are not present, this just adds additional stress to the current team. Ensuring recruitment practices are thorough and fit for purpose, is essential to filling this gap as well as skills assessments within the team and during the recruitment process to ensure the right team member is sourced and then hired.

Boards need to assess, listen, and adjust to the needs of cybersecurity teams and bridge the gap. It means integrating cyber teams into the wider organization, understanding the demands of the roles, and what the skills gaps are within the organization. With knowledge comes power and this is an opportunity for businesses to prioritize cybersecurity to the benefit of their business.

Support for CISOs

To truly connect the board with cybersecurity, CISOs might face challenges. This is due to a lack of awareness and knowledge at the board level and the need for CISOs to clearly report back to the board on the activity of security teams. CISOs also need concrete outcomes from assessments conducted by security teams and clear benchmarking of progress. Failing to connect broader company goals with workforce development in the cybersecurity team can lead to inadequate support and investment in cybersecurity initiatives, leaving the organization vulnerable to sophisticated cyber threats affecting the overall reputation.

There needs to be complete integration of cybersecurity frameworks so there is continuity, understanding, and connection across all levels of the board. CISOs take on a huge amount of responsibility and risk themselves and need to be supported. This can be provided in various ways.

Tabletop exercises for the board level ensure there is a crisis management plan and understanding of how to communicate and react as a business when a cybersecurity breach happens. Having a rapid response plan in place, and testing it out safely, means that businesses are prepared for the worst and feel ready if it happens.

CISOs are on the first line. Security leaders, including CISOs and CIOs, need to lead their organizations through digital transformation, but most importantly, need to deliver value and achieve company goals. To do this successfully, they need to establish a solid collaboration with business leaders, executives, and non-IT decision-makers, driving discussions on the evolving landscape and staying ahead of potential threats. Risk and security are more than ever becoming a distributed C-suite responsibility, not just those of IT management. As the one responsible for both information and security, a CISO must lead the way in meeting security objectives for the greater good of the business and be prepared and supported to do so.

Building a firewall against burnout

Building a firewall needs to be done by the industry. This takes action from businesses, individuals, and national bodies to unite and work together. Recognizing the challenges highlighted across the different levels of the organizations shows the need for the following approach.

- **Maintain skills**
  Without the right skills, professionals will be unable to protect businesses. It is about maintaining the knowledge and the efficiency through continuous improvement, assessment, and practice.

- **Assess skill gaps**
  Businesses need to benchmark team capabilities to understand how well their team aligns with the current requirements of the cybersecurity landscape. Once the gaps are identified, technical leaders can design workforce development plans accordingly.

- **Standardize metrics**
  Organizations find it challenging to compare their teams with industry benchmarks and foster collaboration due to variations in measurement criteria. Universally accepted metrics for assessing cybersecurity capabilities would benefit the industry.

- **Integration of new technologies**
  The introduction of new cybersecurity tools and technologies is frequent. A recent example that has highly impacted the industry can be found in AI, blockchain, and machine learning. Onboarding programs must include training on the latest tools, and existing employees may require continuous development to stay proficient in using new technologies.

- **Transparent hiring expectations**
  Recruitment needs to be specialized so that an individual not only goes into the job role advertised with a clear understanding but also has the key skills to tackle the role successfully.

- **Clear roles and responsibilities**
  Unclear expectations or responsibilities within teams increase business risks. Ensuring individuals know their responsibilities creates clear structures and everyone is confident and capable in their job role.

- **Investment in career development**
  Cybersecurity is known for being relentless, but to maintain performance and engagement across the team, each individual needs a clear career program with goals and objectives for that individual to achieve. Development and upskilling programs are key to maintaining skills, and ensuring that individuals are being fulfilled.

Building a firewall against burnout

Assess business structures
Teams working long hours due to time zone differences is unsustainable. Businesses must adjust logistics, team structure, and procedures to ensure reasonable daily hours. While some tasks may require extended time, the regular workload should be manageable.

Adopt a human-centered approach to cybersecurity
Successful and seamless cybersecurity practices come from high-performing people. For a business to be secure, it takes an elite-performing team. This means understanding and investing in individuals from upskilling but also to creating a connected team that enjoys working together and feels valued.

Reduce pressure with awareness training
Cybersecurity is a business-wide issue and cybersecurity awareness training should be compulsory, company-wide. This ensures that the wider organization can keep an eye on simple processes to protect the organization too.

Integrate cybersecurity into the whole business
Cybersecurity and tech leaders should attend head-of-department and C-level meetings to flag issues more easily and connect teams better to the business. Cybersecurity needs to be on the board's agenda and prioritized. CISOs have a huge amount of pressure to protect the whole business from data to finances.

Tackle stress, fatigue, and burnout
Cybersecurity is a demanding field. Individuals need to be encouraged to take time off, look after themselves, and have an external support network that is there to ease pressure and listen. This needs to be an attitude fed down from the top of the business.

> In my opinion, there’s no one size fits all, but for me what works is making sure you take breaks when you need them. You’re not going to fall behind if you give yourself a day or two where you don’t think about cybersecurity to focus on what makes you happy.

Chrisostomos Kollaras, Penetration Tester at EY

Proactive steps forward

The life of a modern cyber professional is not about individual ability or certifications. They also require the capability to match the existing processes with concrete business outcomes, and an environment fostering career progression and well-being. In addition, businesses need to invest in people's careers, development, and well-being. This will unlock every team's full cybersecurity performance and thus lead to a better security posture.

Hack The Box's Cyber Performance Center redefines cyber performance. It provides a platform for business and tech leaders to develop their workforce with plans aligned with organizational objectives, and for teams, professionals, and students to grow.

Hack The Box's methodology aligns cybersecurity goals with business objectives through the People, Process, Technology framework:

- **People:** Provide comprehensive career path programs for individuals to develop their skills and knowledge continuously. This includes technical training on tools and technologies, as well as soft skills training on communication, teamwork, and problem-solving.

- **Process:** Integrate cybersecurity workforce development into existing processes, such as incident response and risk management. Conduct regular tabletop exercises and simulations to practice responding to cyber incidents.

- **Technology:** Use cutting-edge upskilling courses, labs, and cyber range scenarios equipped with simulated networks, systems, and attack vectors to build hands-on experience in a controlled environment that avoids harming production systems.

This methodology positively impacts business metrics and cyber resilience, through a concrete cyber performance program. Unlike traditional training methods, Hack The Box provides an all-in-one platform combining ability, business management, and human focus to drive performance, addressing industry challenges like skills gaps, and burnout. The platform features are designed to oversee skills development and analyze potential gaps that could cost real dollars to businesses.

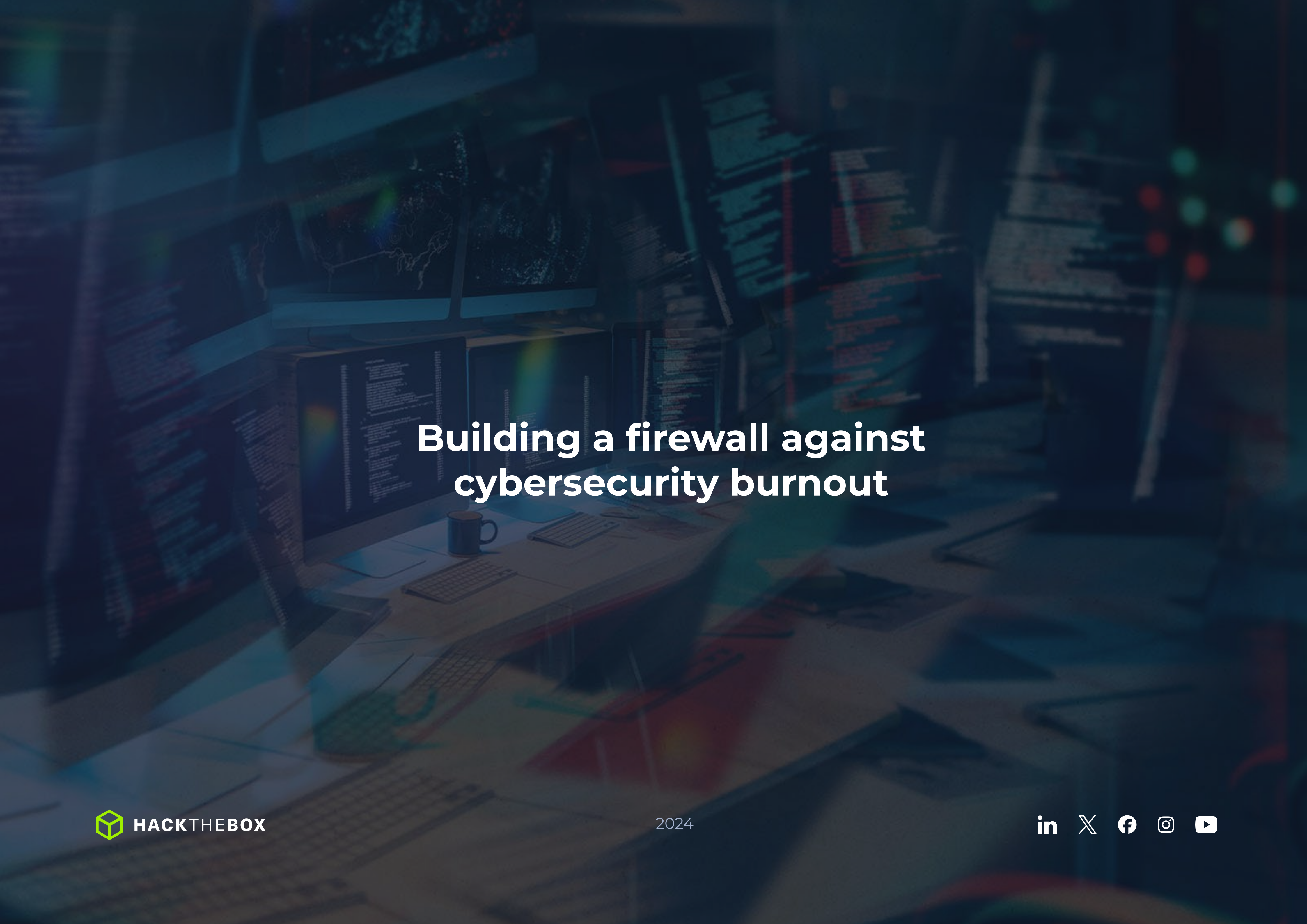
About Hack The Box

Hack The Box is the Cyber Performance Center with the mission to provide a human-first platform to create and maintain high-performing cybersecurity individuals and organizations.

Hack The Box is the only platform that unites upskilling, workforce development, and the human focus in the cybersecurity industry, and it's trusted by organizations worldwide for driving their teams to peak performance. Offering an all-in-one environment for continuous growth, assessment, and recruitment, Hack The Box provides solutions for all cybersecurity domains.

Launched in 2017, Hack The Box brings together the largest global cybersecurity community of more than 2.8 million platform members. Rapidly growing its international footprint and reach, Hack The Box is headquartered in the UK, with additional offices in the US, Australia, and Greece.

For more information, please visit
hackthebox.com



Building a firewall against cybersecurity burnout

HACKTHEBOX

2024