HACKTHEBOX

SECURING THE FUTURE OF CYBERSECURITY

From classroom — to every career stage

Table of contents

From classroom to career

HARIS PYLARINOS
CEO & Founder
@ Hack The Box

The cybersecurity skills gap and talent shortage are undeniable. It is an ongoing topic on the agenda of almost every business. Protecting organizations against advanced and destructive cybersecurity threats is critical, and IT and security teams are under increasing pressure to safeguard a business successfully.

However, our research reveals that to build successful security teams, we need to revolutionize the entire career path for cybersecurity professionals. Cybersecurity and IT professionals reveal that the education system needs much more hands-on experience to ensure it is cultivating a hacker mindset. In addition, current recruitment processes often inadvertently result in the rejection or avoidance of highly qualified talent, as recruiters may prioritize the wrong qualifications in their assessment.

In this rapidly moving, ever-evolving threat landscape, security teams need to be ahead of all current techniques and skills as it gives practitioners the expertise they need to proactively identify and mitigate vulnerabilities before attackers can exploit them. Incorporating hands-on learning into university curriculums to bridge the gap between academic knowledge and practical skills, redefining recruitment practices, and investing in continuous workforce upskilling is essential. Our research also shows how AI will impact the cybersecurity industry and how we need to prepare workers for this accelerating future of sophisticated attacks. Perseverance and outside-the-box thinking are the core hacking skills that form true experts, not memorizing handbooks and blindly following instructions. This needs to be fostered from the beginning and throughout a career path to ensure success.

It is time for us to unite departments and industries to create a force to be reckoned with - a secure future for cybersecurity professionals from the classroom to every career stage. The future of successful cybersecurity lies in the hands of the next generation.

Methodology: Hack The Box, commissioned an independent market research company, Censuswide, to survey a sample of 3,000 IT and cybersecurity professionals in the UK and the US between 20th October and 30th October 2023. Unless stated otherwise, all figures were drawn from this poll.

Key takeaways

95%

believe their organization understands the importance of cybersecurity and the skills required to mitigate risks effectively

64%

feel that current recruitment processes fail to effectively evaluate practical skills in addressing evolving cyber threats

78%

say that traditional university cybersecurity education is not adequately preparing graduates for countering evolving cybercriminal tactics

90%

say cybersecurity and computer science graduates need to be prepared with hands-on experience before their first role in cybersecurity to be successful

University curriculums & the modern work landscape

Education is the first step in the cybersecurity and IT professional pathway. 90% of respondents say cybersecurity and computer science graduates need to be prepared with hands-on experience before their first role in cybersecurity to be successful. Yet, there are two issues revealed in our research.

Current education systems should increase practical, real-life learning experiences within the syllabus to prepare new recruits for the role.

Overall, 78% of respondents expressed concerns that traditional university education in cybersecurity does not fully equip graduates with the practical skills needed to effectively combat the evolving and sophisticated tactics that cyber-criminals employ. This sentiment is even more pronounced in the UK, where it rises to 83%, and in the US, where 74% share this perspective.

University curriculums do not include enough hands-on experience for students to ensure they are prepared for future IT and cybersecurity roles. Yet, this is essential for roles to be filled successfully.

UNIVERSITY OF SOUTH FLORIDA

Marbin Pazos Revilla, Assistant Professor of Instruction and Systems Administrator at the University of South Florida, is integrating Hack The Box's platform into the curriculum and says:

"

We needed a common and effective platform that every student, regardless of their background or abilities, could navigate and build the skills they need to succeed in the cybersecurity industry, this is critical in today's landscape. Today's students need to have a rich experiential learning environment, with content reflecting the reality students will face in their future cybersecurity career roles.

Hack The Box's recent research points out the importance of integrating practical learning into the university curriculum. We see first-hand that Hack The Box positively impacts the student's ability. The atmosphere in the classroom changes once you put the challenge in front of them, and you can feel the energy and watch the collaboration and interactions take place naturally. This needs to be commonplace for students around the world.

Since integrating HTB in August 2022, we've seen a remarkable spike in student interest and engagement. The platform's effectiveness is evident in reduced preparation time, improved student skills in under six months, and alignment with current industry trends. It's not just a tool; it's a catalyst for success, fostering a dynamic learning environment at USF.

Sector insights into hands-on university curriculums

For IT and security businesses, the education system is not supporting students enough with practical skills to be prepared for the sophisticated attacks used by cyber-criminals. In contrast, some specific industries, such as healthcare and government organizations, view this as less of an issue.

Fig.1: According to industry sectors, "A traditional university education in cybersecurity is not doing enough to practically prepare graduates for the evolving and sophisticated tactics cyber-criminals use"

Business size insights into hands-on university curriculums

In addition, the need for graduates to have hands-on experience is even more pronounced for mid to large-sized organizations. It is key that graduates can access all businesses and feel prepared for the role they secure, particularly so they retain their role and flourish.

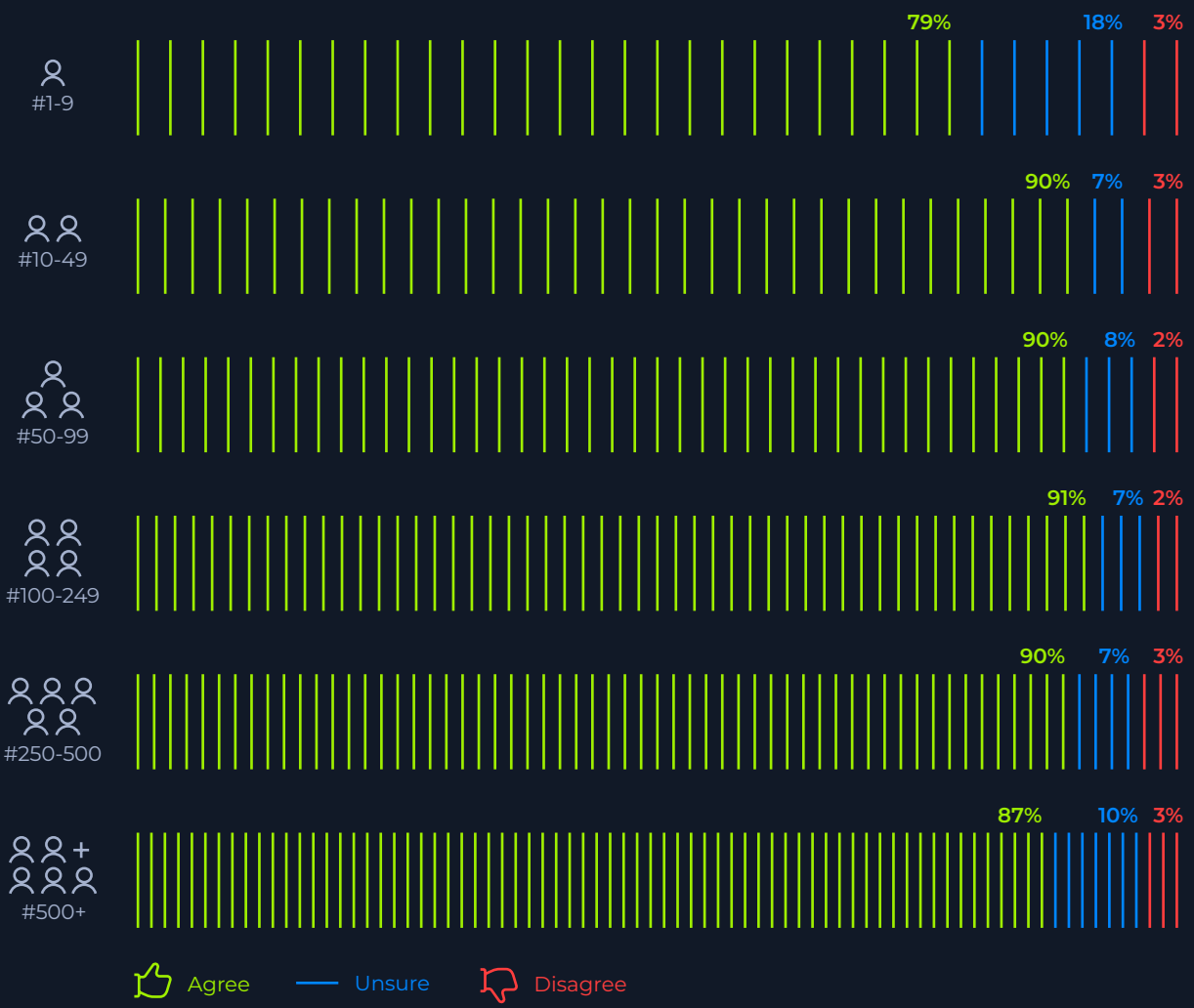


Fig.2: According to different business sizes, “Cybersecurity and computer science graduates need to be prepared with hands-on experience before their first role in cybersecurity to be successful”

Cybersecurity team insights into hands-on university curriculums

Compliance and risk management see the highest need for hands-on learning experiences. This is similar for general IT staff and offensive security teams, demonstrating the overall need for hands-on training before a graduate explores a new role in cybersecurity. This shows that there is an overall need for a more prepared workforce.

Fig.3: According to departments, “Cybersecurity and computer science graduates need to be prepared with hands-on experience before their first role in cybersecurity to be successful”

Age group insights into hands-on university curriculums

The youngest of the age groups, 18-24 year olds, who are newly qualified, are the ones who believe that traditional education is not doing enough to prepare them for the world of cybersecurity practically. These individuals have just left university, with the closest insight to the latest university syllabus, so they provide accurate insight into the need for practical learning within the education system.

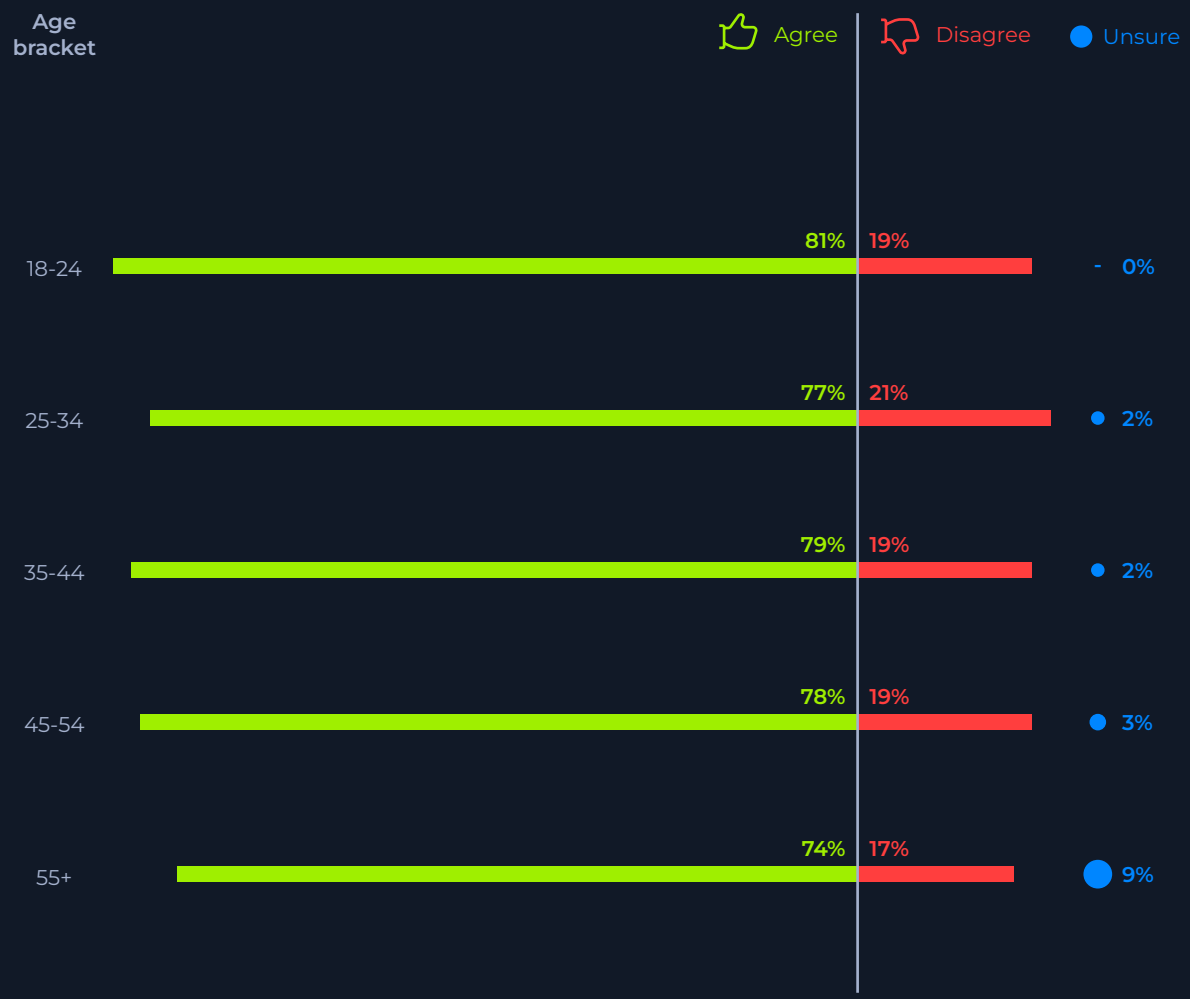


Fig.4: According to age groups, “A traditional university education in cybersecurity is not doing enough to practically prepare graduates for the evolving and sophisticated tactics cyber-criminals use”

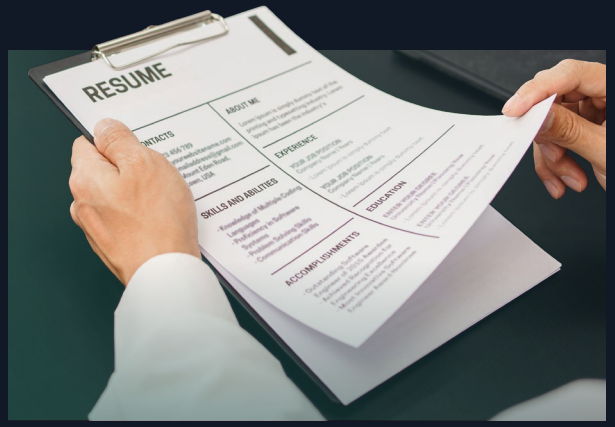
Finding the value in a candidate's CV

According to our research, hiring new recruits is a challenge when organizations need to find the right talent for the role, someone who is going to fit into the team and be able to hit the ground running. Ensuring the right candidates are filtered through to the interview and hiring stage is essential for success.

There seems to be an 'expectations gap' in cybersecurity recruitment, which assumes that applicants who have the necessary experience but not the qualifications are unsuitable. This gap is leading to talented individuals not being included in the shortlist for a role.

In our report, respondents highlighted that when searching for their first permanent role within the industry since graduation, the areas of most value to employers were being overlooked. For example, the most valuable part of a CV, based on their point of view, is cybersecurity-specific certifications, which demonstrates their practical experience and shows they can deliver on the role advertised. Yet, the recruiters do not seem to consider this. In comparison, the area of least value overall was a university degree, according to respondents.

According to the 'Cyber security skills in the UK labor market 2022' study from the UK Government, "employers continue to place a strong emphasis on applicants having bachelor's degrees or higher qualifications. 90% of employers expect a minimum of a bachelor's level degree (in a related subject) for core cybersecurity roles." In addition, in the US, a 2020 study from Northern Michigan University states that 60% of entry-level cybersecurity jobs require a college or university degree in a related

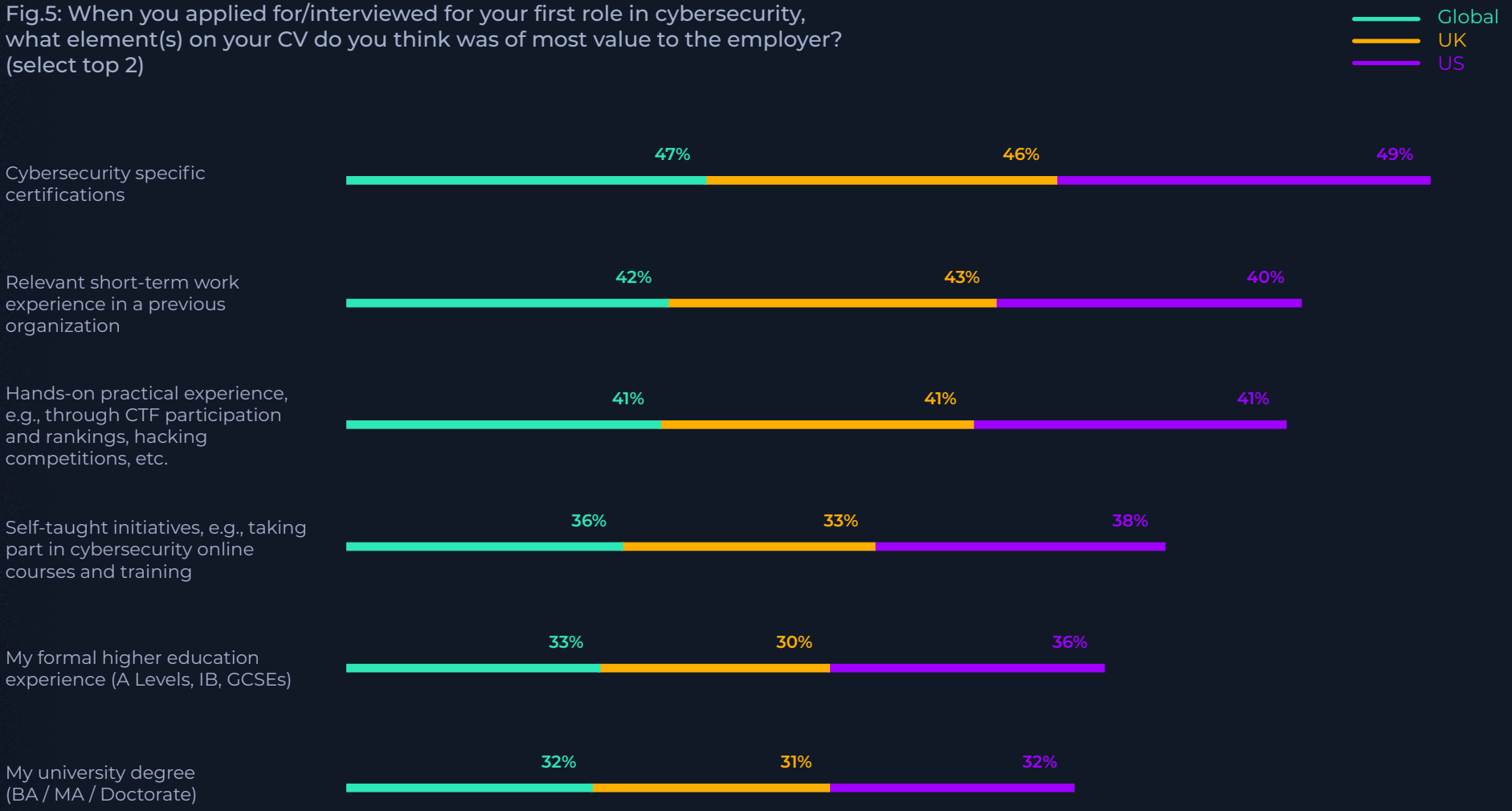


field. Requiring a university degree for entry-level roles rules out highly talented candidates with practical skills and experience in the job field.

The industry calls for businesses to recognize that a CV needs to be considered across all areas, not just the traditional education system. Individuals with proven practical experience are highly beneficial to an organization looking to fill a role with a capable and talented employee. Many overlooked individuals are suitable for the role.

IT & cybersecurity professional insights

Fig.5: When you applied for/interviewed for your first role in cybersecurity, what element(s) on your CV do you think was of most value to the employer? (select top 2)



Experience level insights into a traditional CV

Those in more junior job roles, such as entry-level and intermediate, place the highest value for the employer on self-taught initiatives and practical experience through CTF participation and hacking competitions. This shows businesses that employees need to be prepared for the workplace, as well as their drive to improve, learn, and develop as individuals.

Cybersecurity and IT professionals are innovators and problem solvers and need to keep ahead of the latest trends. The practical learning and hunger to develop greatly benefit employers looking to recruit staff that will thrive and deliver results.

Fig.6: According to job title, "When you applied for/interviewed for your first role in cybersecurity, what element(s) on your CV do you think was of most value to the employer?" (select top 2)

	Business Owner	C-Level Exec	Senior Management	Middle Management	Intermediate	Entry level
Cybersecurity specific certifications	51%	47%	55%	40%	33%	28%
Relevant short-term work experience in a previous organization	38%	40%	43%	48%	38%	15%
Hands-on practical experience e.g., through CTF participation & rankings, hacking competitions, etc.	40%	41%	41%	44%	32%	36%
Self-taught initiatives e.g., taking part in cybersecurity online courses & training	37%	40%	34%	29%	34%	38%
My formal higher education experience (A Levels, IB, GCSEs)	33%	40%	31%	29%	21%	21%
My university degree (BA / MA / Doctorate)	27%	37%	27%	28%	33%	26%

Redefining recruitment

Solutions to the recruitment challenge lie in ensuring the recruitment process considers whether candidates have the practical skills to immerse themselves into their new role effectively and efficiently.

Recruiting in the cybersecurity space is very specific based on the needs of a business and there are nuances to the talent needed for different industries. For example, there are different skill sets as well as business priorities that are important to take into account for financial services or software vendors.

Businesses need to utilize the right tools throughout the entire recruitment process, from assessment tools used during the recruitment process and listing jobs where the most promising and proactive candidates will apply for the role. Businesses and recruiters also need to adopt a more creative approach to assessing candidates.

Current cybersecurity and IT teams are calling for the recruitment process to adapt, including:

- **Collaboration and knowledge sharing:** Recruiters, HR, and talent teams to work with the cybersecurity industry professionals to develop effective recruitment strategies and adopt a more creative approach to assessing candidates.

- **Shifting to a focus on industry certification:** More emphasis on the industry certifications and practical upskilling methods candidates have obtained (e.g. CTF competitions) to avoid overlooking external certification and skills outside University degrees that can be valuable to businesses.

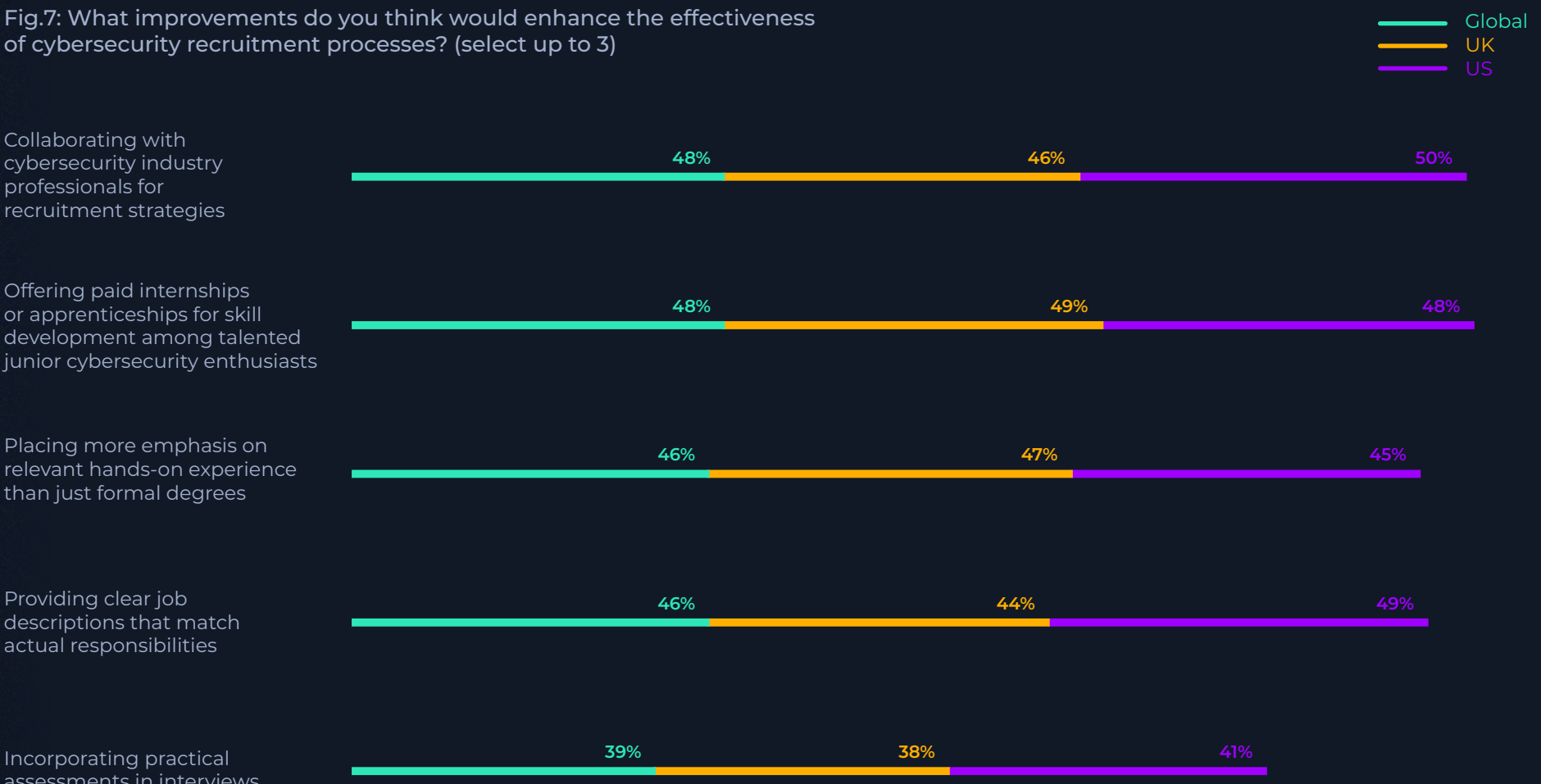
- **Nurturing talent:** Businesses to encourage internships, apprenticeships, and practical learning experiences to nurture the skills of young cybersecurity and IT talent.

- **Promoting practical learning:** Incorporation of practical assessment processes as part of the recruitment process so candidates can showcase their expertise and mindset and ensure they are the right fit for the role.

- **Accurate adverts:** Clear job descriptions that accurately reflect the actual responsibilities of the role to ensure an appropriate individual is hired for the role.

Cybersecurity and IT professionals: Improving recruitment

Fig.7: What improvements do you think would enhance the effectiveness of cybersecurity recruitment processes? (select up to 3)



Sector insights into recruitment

According to industry sectors, the perception in the security and IT/Telecoms industries is that recruitment processes do not effectively evaluate a candidate's practical skills. This is in contrast to legal industries, where the perception is that recruitment processes work.

With the need for the cybersecurity industry to be a step ahead, this comparison shows the importance of ensuring recruitment processes effectively evaluate skills across each industry. As telecoms is part of a country's critical infrastructure, remedying these issues is essential. Solutions need to be industry-specific and not a blanket approach to ensure recruitment works for all sectors. Recruitment into these industries needs to be revisited as a priority.

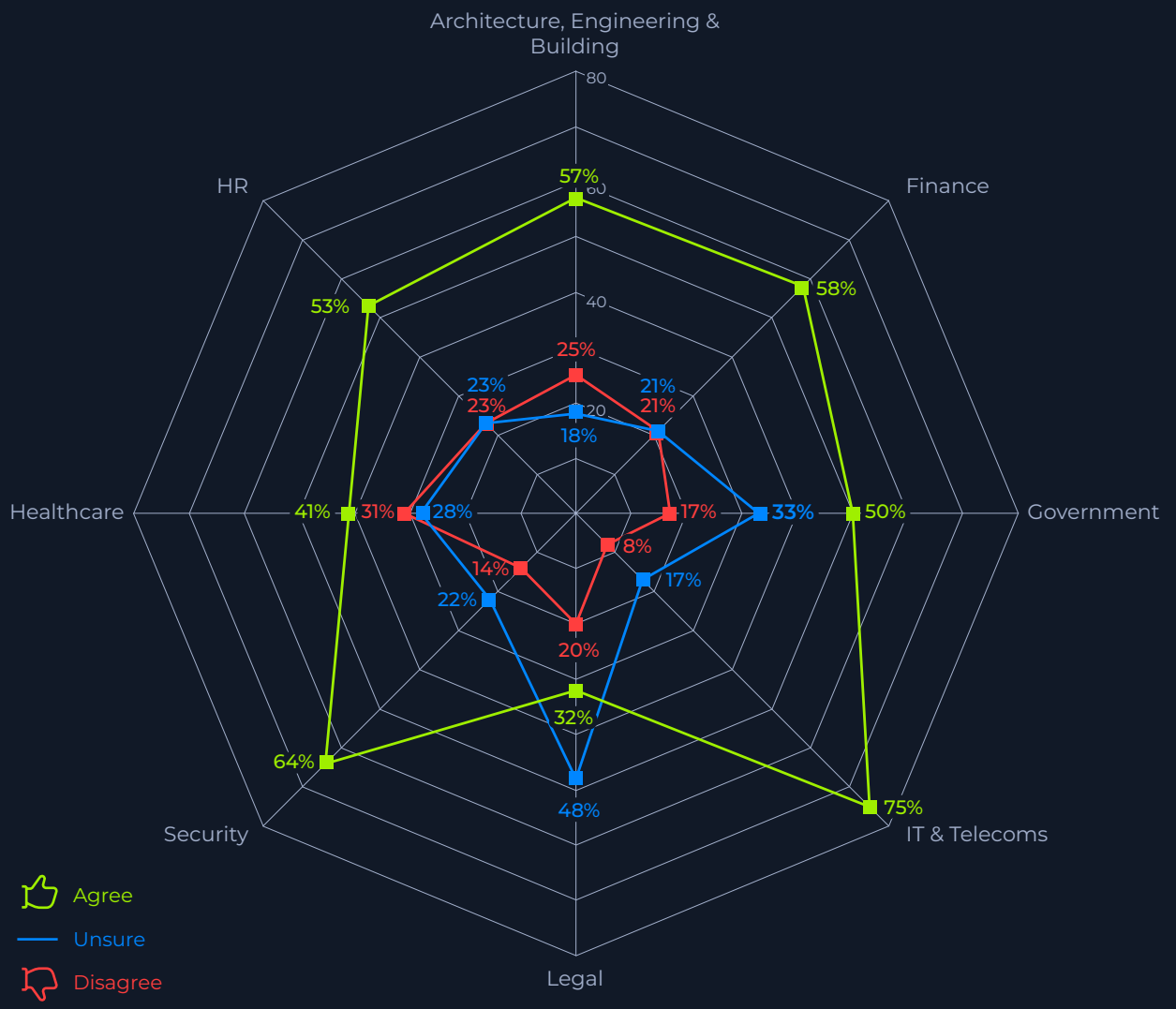


Fig.8: According to industry sector, to what extent do you agree with "Current cyber recruitment processes do not effectively evaluate candidates for their practical skills in addressing evolving cyber threats"

Ongoing upskilling & career investment

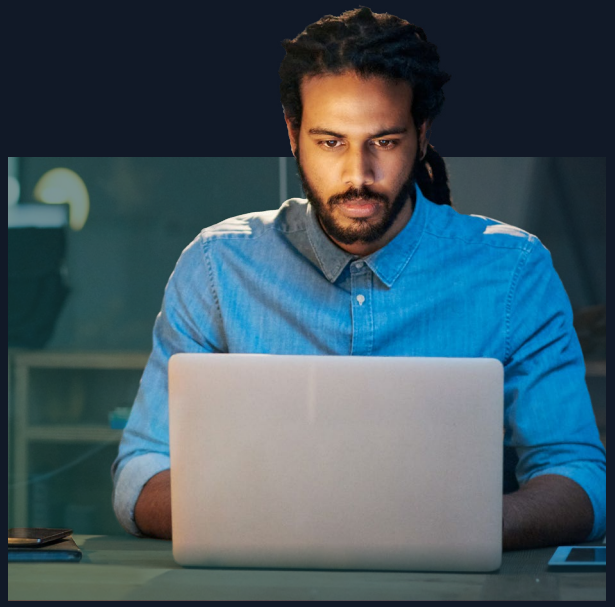
With a 600% increase in cybercrime since the COVID-19 pandemic and the average cost of security breaches in 2022 to be $4.35 million, businesses are focused on protecting their systems now more than ever.

According to our latest survey, 95% say their organization understands the importance of cybersecurity and the skills required to mitigate risks effectively. Businesses are investing in their upskilling programs and taking this seriously, with 96% of cybersecurity and IT professionals having been offered cyber upskilling programs in 2023.

However, this perception shifts between senior decision-makers and entry-level recruits, with improvements to be made for new recruits and less experienced team members. C-suite leaders think their teams have the skills needed. However, the more junior members of the team and those actively protecting the business are more concerned, showing a need for assessing the skills needed within the team and implementing the training necessary.

With less support, entry-level candidates can impact retention and skill development and put organizations at higher risk of breaches if entry-level roles are not continuously upskilled at the rate of other team members. Cybersecurity will continue to have a learning gap if this is not solved, and it is essential for continued investment. Continuous workforce development and ongoing upskilling are essential to retaining talent, staying protected, and mitigating risks.

Access to ongoing upskilling programs is essential for the teams



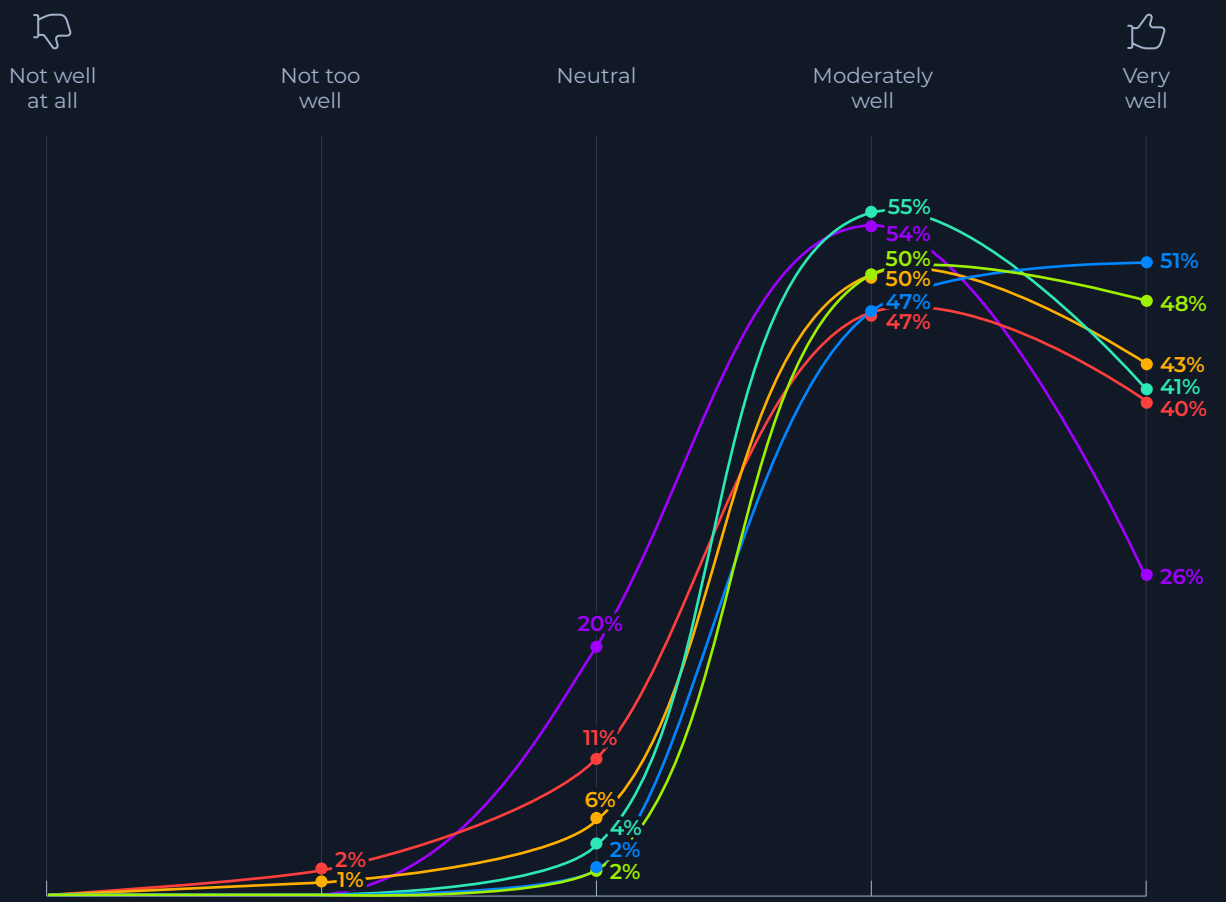
to be supported and updated with the latest tools and techniques. 82% of respondents said there is plenty of financial investment in their department to protect their organization from cyber threats. However, investing in the right tool to ensure the team feels confident, capable, and ahead of the latest trends is essential. Assessing what is needed and where to source effective upskilling training is essential.

The importance of mitigating risk

Building high performing teams is essential to success and ensuring new recruits are supported, trained and provided continuous upskilling opportunities is essential for employee wellbeing, morale and retention.

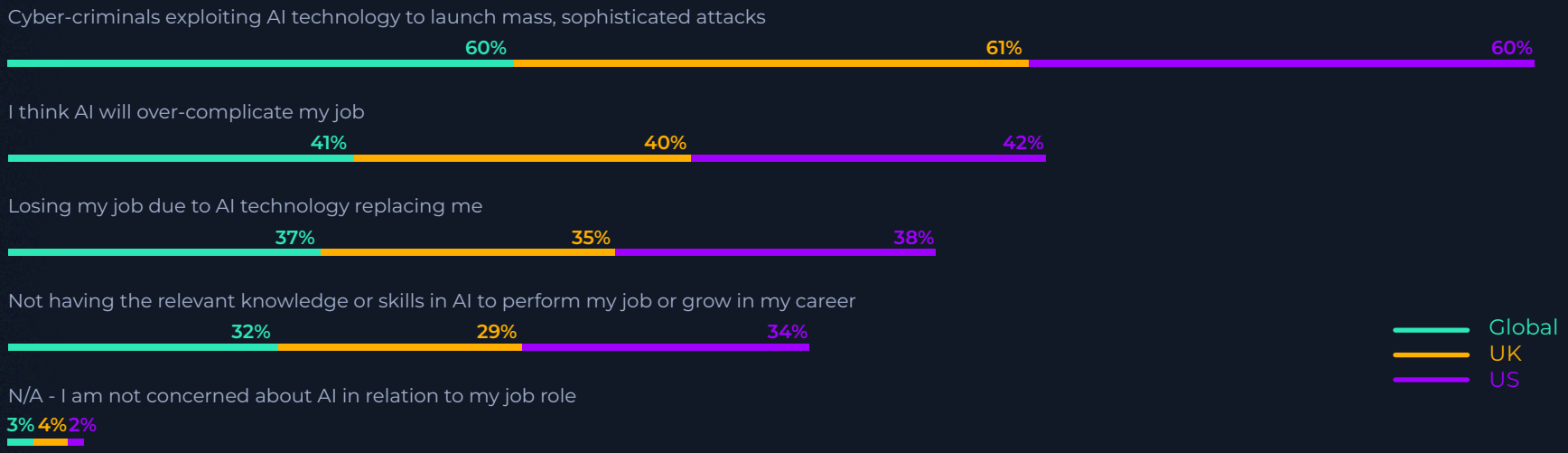
In addition, only 70% of cybersecurity and IT professionals have been offered cybersecurity training in the last year and are currently taking part in upskilling. The split between the UK reduces to 68% in the UK and 72% in the US. A high percentage of the workforce still needs to be provided with current upskilling programs.

Fig.9: According to seniority, how well does your organization understand the importance of cybersecurity and the skills required to mitigate risks effectively?



The AI dilemma

Fig. 10: What concerns you the most about the rapid development of AI in relation to your job role, if anything? (Select top 2)



The cybersecurity landscape is constantly evolving. In this report, 60% of professionals express concern about cyber criminals exploiting AI technology to launch large-scale, sophisticated attacks. The landscape is changing for cybersecurity, and individuals at every stage of their careers need to ensure they stay ahead of the latest risks and threats.

This data shows:

- **41%** believe that AI may overcomplicate their job roles
- **37%** are concerned about job security, fearing that AI technology could replace their positions
- **32%** fear not possessing the necessary knowledge or skills in AI to perform their job or advance in their careers effectively

It is clear from this data that to create a successful and motivated workforce, businesses need to invest in ongoing learning and upskilling with top-notch tools and resources for their cybersecurity and IT teams. Particularly in the face of growing attacks and growing risks, such as the growth in AI.

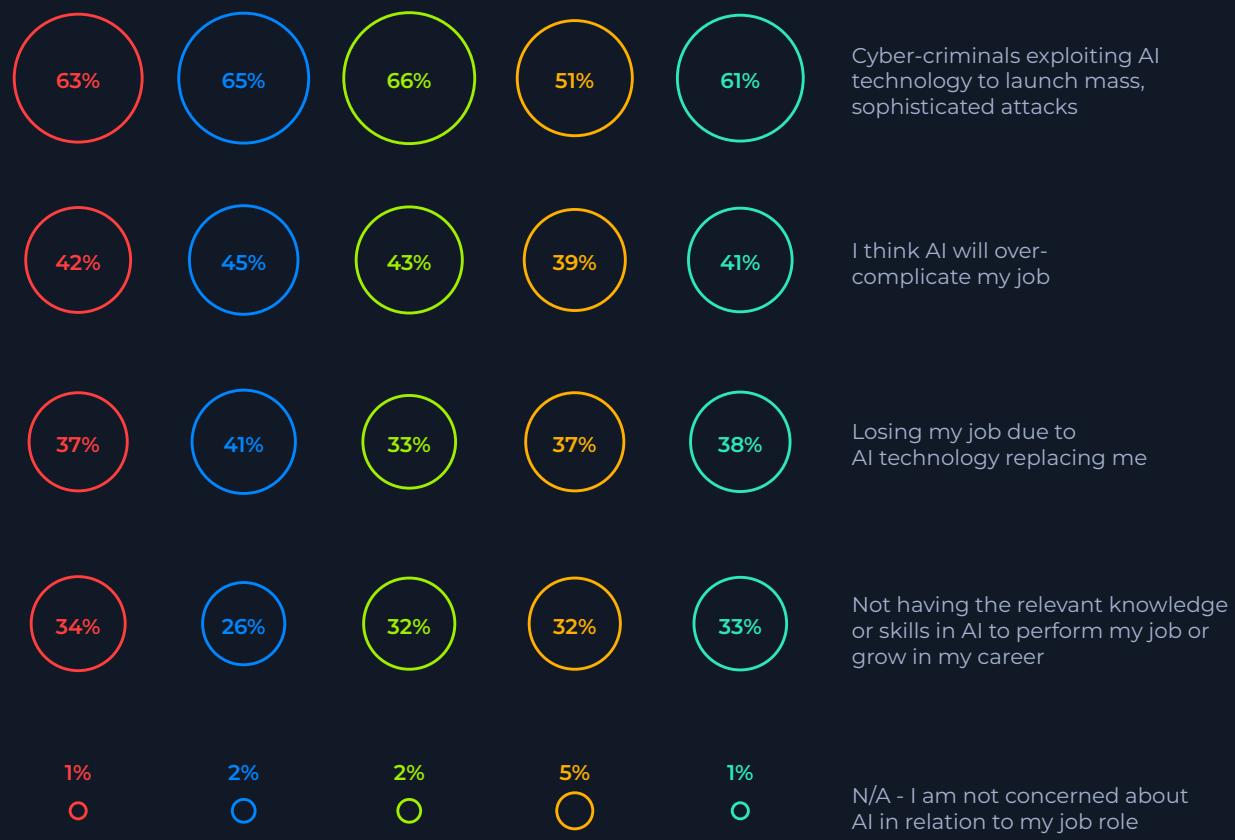
Department insight on AI development

All departments have the same highest concern for the risk of mass, sophisticated attacks, demonstrating none of these departments are prepared for possible AI attacks. This needs remedying with ongoing and cohesive training in this area.

Defensive teams believe they are at the highest risk of losing their jobs due to AI replacing them, demonstrating the value they place on other departments. This could result in movement between departments as AI development accelerates to ensure the skills shortage in this department does not continue to grow.

Red team / offensive security
Blue team / defensive security
Compliance & risk management team
General IT staff
Security awareness & training team

Fig. 11: According to department, what concerns you the most about the rapid development of AI in relation to your job role, if anything? (Select top 2)



Supporting our front-line workers

Our research demonstrates that the career pathway for cybersecurity professionals is not smooth and it is essential that businesses reconsider how teams are recruited, taught, upskilled, and developed to create a powerful team to be reckoned with. Some of the core issues currently hindering cybersecurity career development and impacting the skills shortage in the industry are due to:

Lack of relevant knowledge from university degrees

78% feel that universities are not doing enough to prepare students for the modern cyber workforce and that education formats need to adapt.

➜ Hands-on learning solutions need to provide advanced skills development plans for students that can be easily integrated with a standard syllabus and mapped against the most relevant industry frameworks.

Outdated recruitment processes

80% of global cybersecurity professionals believe that the high barriers to entry in the field are primarily rooted in the lack of value placed on practical skills, and the traditional CV needs to be adjusted.

➜ Access the right talent by sourcing talent from a community of active professionals looking for their next career move to invest in hiring the right talent from the right place.

Lack of talent assessment practices

A substantial 64% of individuals within the cyber industry assert that existing recruitment processes inadequately assess candidates for their practical skills in addressing ever-evolving cyber threats and businesses need to use creative assessment tools to ensure the right individuals are hired.

➜ Whether hiring a SOC Analyst, Bug Bounty Hunter, or Penetration Tester, assessments need to be tailored thoughtfully to assess the exact skills demanded by the industry.

Sheffield Hallam University

Sina Pournouri, Course Leader of MSc Cybersecurity at Sheffield Hallam University says:

"

We chose Hack The Box as a partner specifically for modules like Ethical Hacking and Penetration Testing to address the lack of specialized laboratories for these areas. Not only do students gain access to the labs anytime, anywhere, but they can also execute instructions regardless of their PC or laptop specifications, courtesy of Hack The Box's Pwnbox.

An added benefit of using HTB is the access to a variety of vulnerable machines, continually expanding and refreshing our training resources. This exposure acquaints students with more real-world, industry-related case studies.

Since incorporating Hack The Box, we've updated our module syllabi to align more closely with current trends. Previously limited in the number of vulnerable machines available, now, thanks to Hack The Box, we can operate on a significantly larger pool of machines during lab sessions. The tagging system for identifying suitable machines has greatly aided in lab preparation and teaching.

Advice for businesses looking to upskill their cybersecurity & IT teams

JAMES HOOKER
CTO & Co-Founder
@ Hack The Box

Cybersecurity is a growing industry, and it is essential to be creative and look ahead to what the future holds. Undoubtedly, we are seeing a growth in threats and a growth in skills shortage. Therefore, it is paramount for organizations to consider how they are fostering morale, well-being, and boosting talent in this sector. Our cybersecurity and IT professionals need to be inspired and challenged, and they need a transformative, creative, and engaging approach to upskilling to make this happen throughout all career pathways. Universities need to equip their students with practical skills, preparing them for the demands of the professional world. CVs need to be revisited, and recruitment needs to happen using creative assessment tools specific to the job role. Building high-performing teams and an inspiring culture, we set businesses and individuals up for success.

About Hack The Box

Launched in 2017, Hack The Box brings together the largest global cybersecurity community of more than 2.5m platform members and is on a mission to create and connect cyber-ready humans and organizations through highly engaging hacking experiences that cultivate out-of-the-box thinking.

Offering a fully guided and exploratory skills development environment, Hack The Box is the ideal solution for cybersecurity professionals and organizations to continuously enhance their cyber-attack readiness by improving their red, blue, and purple team capabilities.

Rapidly growing its international footprint and reach, Hack The Box is headquartered in the UK, with additional offices in Greece and the US.

For more information, please visit hackthebox.com

2.5m
Hack The Box members

1,050+
Machines, challenges & Sherlocks

1.5k+
Organizations using Hack The Box

990+
Universities enrolled

1,360+
CTFs & meetups

Trusted by the world's most ambitious CyberSec teams, incl. **Fortune 500** and **Fortune 1000** companies

Deloitte. TOYOTA EA SPORTS Booz Allen PUMA

Contact us

We are the leading gamified cybersecurity upskilling, certification, and talent assessment platform enabling individuals, businesses, government institutions, and universities to sharpen their offensive and defensive security expertise.

For more information, contact:
pr@hackthebox.com

Securing the future of cybersecurity

From classroom to every career stage

HACKTHEBOX

2024