HAYS Working for your tomorrow

GLOBAL **CYBER SECURITY** REPORT 2024

Beyond traditional cyber talent

Experts in
Technology

CONTENTS

Introduction

THE DEMAND FOR CYBER SKILLS

Cybercrime is one of the greatest risks we face in our modern era. No organisation, public or private, large or small, can afford to underestimate the threat of cybercrime in 2024. Cyberattacks will cost the world an estimated $9.5 trillion this year, while leaving a lasting impact on the reputation and future operations of any organisation that fails to fight back. We must win this fight!

How do we beat cybercrime? With people. We must engage the boardroom, maximise technology, and leverage human capital to win. The common thread is people. Highly motivated, talented and innovative people. Finding and retaining the right people, with the right skills, focused on the right technology is essential for businesses today. There are an estimated 3.5 million cyber security vacancies worldwide. At Hays, we see the impact of this deficit daily. Ready-made talent is scarce, and technology is advancing at an unprecedented rate. New technology brings innovation as well as increased risks and vulnerabilities. More technology in our spaces means more criminals in our spaces. We must fight back, but cyber security professionals struggle to keep their skills up to date.

Yesterday's paradigms will not bring tomorrow's results. We must understand where we are today with an eye on tomorrow to effectively chart our path into the future. That's why it is a great privilege to introduce another Hays Annual Global Cyber Security Report, with insights from over 1,000 CISOs and cyber security leaders worldwide.

While over half of respondents reported growing their cyber security team last year, leaders are more concerned about their budgets than 12 months ago – with investment in headcount being the area of most concern. Today's dynamic geopolitical and economic climate has impacted spending for over 75% of our respondents, and employers must look beyond salary increases to attract cyber talent. Remote and hybrid working opportunities, as well as greater flexibility, are becoming increasingly important.

It is vital that we work together to build a pipeline of cyber security talent with the right skills to solve tomorrow's challenges. Many of you have recognised and explored non-traditional cyber talent as a solution, i.e. those with neither formal education nor experience in the field. However, we can do even more. Data from our survey suggests that employers worldwide aren't unlocking the full potential of this untapped talent pool. The root cause: lack of adequate investment in dedicated training and development, and limited flexibility of hiring departments to look beyond typical hiring procedures.

Simultaneously, there is a need to leverage the rapid evolution we're witnessing in Artificial Intelligence. While our respondents believe AI can support their security capabilities, there is hesitation over its implementation as a tool, or potential co-worker, for the workforce to utilise.

Throughout our report, you'll find comments from experts and cyber security thought leaders at Hays who are working tirelessly on the front lines to help solve these challenges. I'm also honoured to share the insights of cyber security leaders from world-renowned organisations who are dedicated to winning this fight against cybercrime. Their contributions are priceless!

While over half of respondents reported growing their cyber security team last year, leaders are more concerned over their budget than 12 months ago

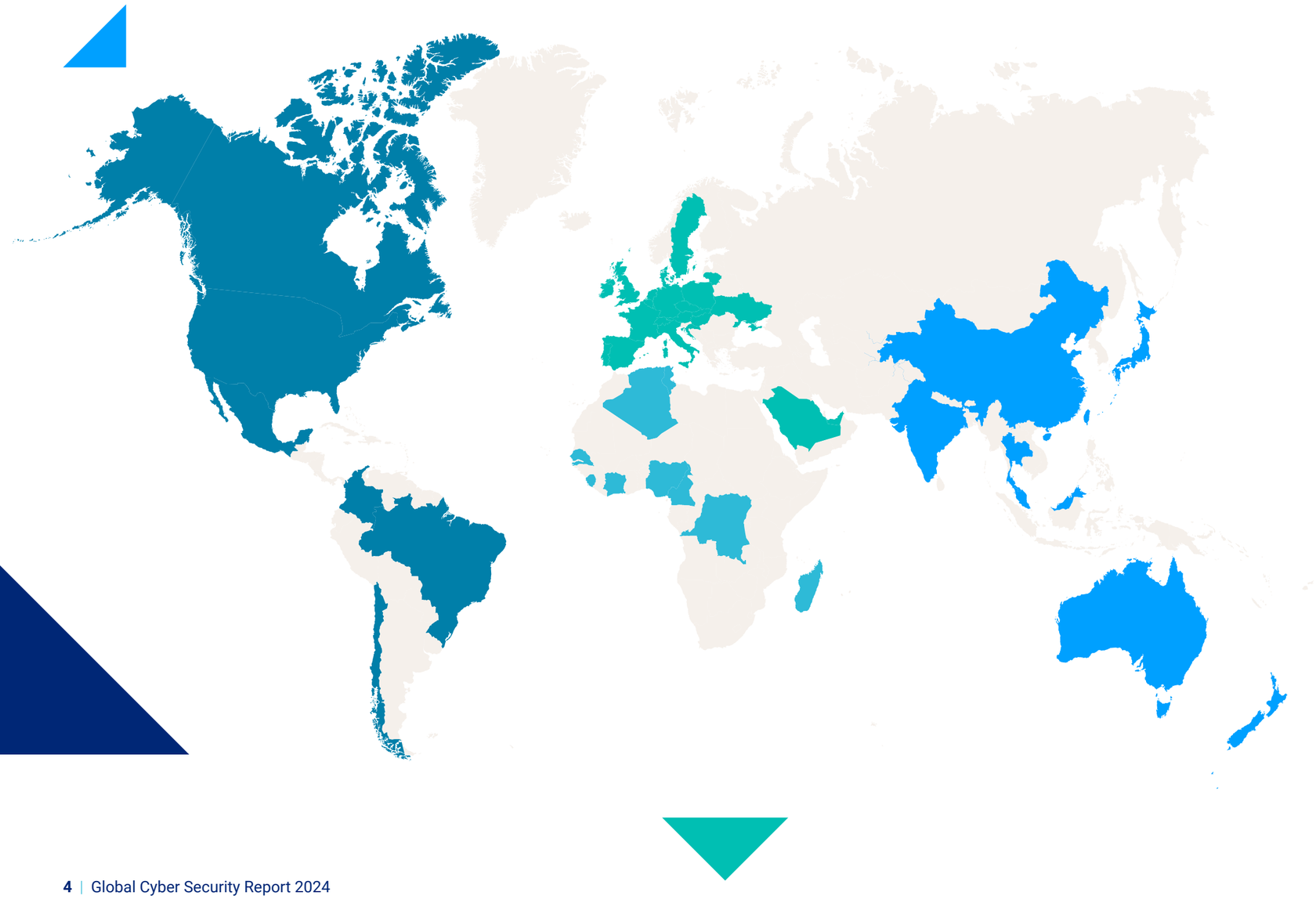
We trust that the results of our survey, as well as the advice from experts both inside and outside of Hays, will benefit you as you diligently fight cybercrime on a daily basis. No one can survive as an island of isolation. We are in this fight together and we are in it to win it.

A special note of appreciation goes out to all our contributors, as well as our diverse pool of survey respondents. Without your willingness to share your considerable experiences and expertise, we wouldn't have been able to offer these valuable insights. Thank you!

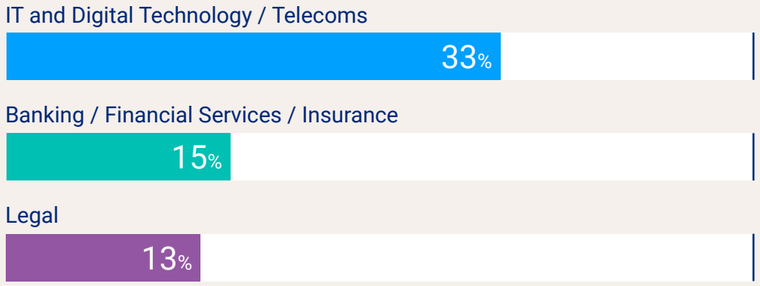
Michael Beaupre
Head of Cyber Security Solutions, Hays CEMEA

ABOUT THE **SURVEY**

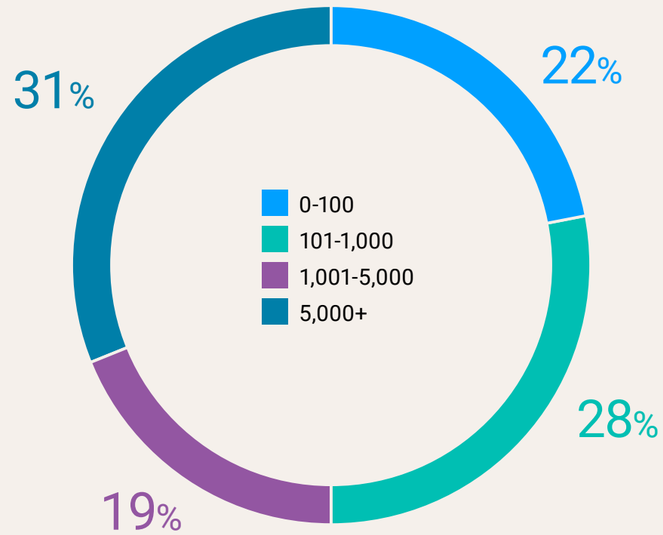
Our survey was completed in late 2023 by over **1,000 cyber security leaders from 47 countries worldwide**. Our respondents, contacted through our global database and via direct request, have all shared how their organisations are currently approaching the recruitment and retention of qualified cyber staff, and revealed how they expect AI to impact their work in the near-to-medium term, including providing insights into plans for investment in security and human resources.



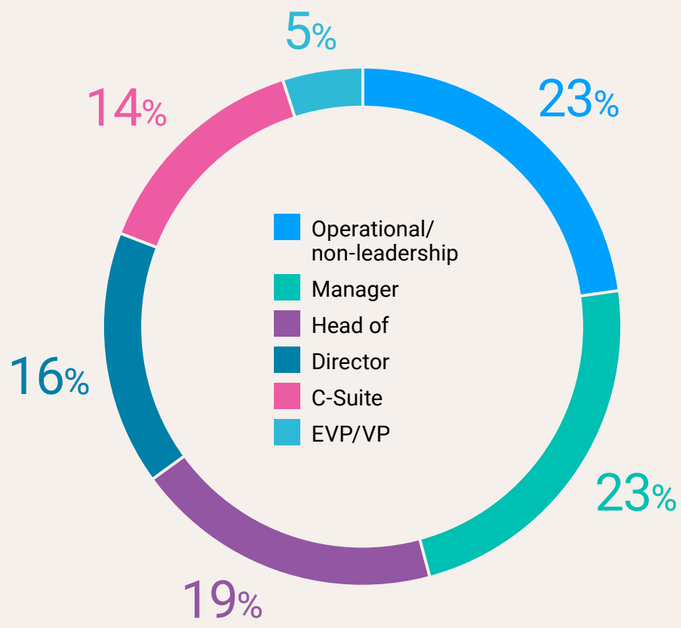
Top business sectors our respondents work in



Employees at our respondents' organisations



Seniority level of our respondents



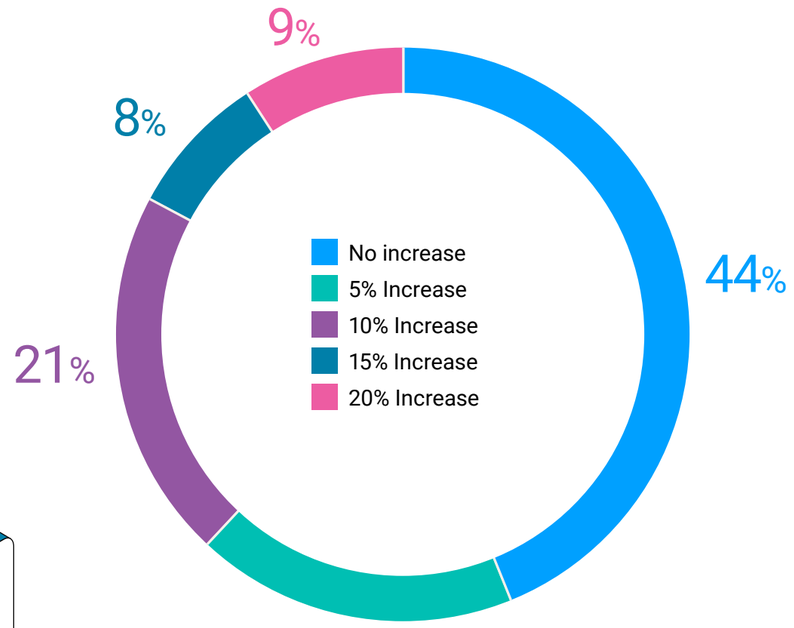
THE CHALLENGE: **HIRING & RETAINING** SKILLED TALENT **UNDER BUDGET RESTRAINTS**

Last year's report uncovered that over half of respondents were struggling to attract the right talent. Twelve months on, the landscape hasn't shifted: 61% of respondents do not rate their ability to attract cyber talent highly.

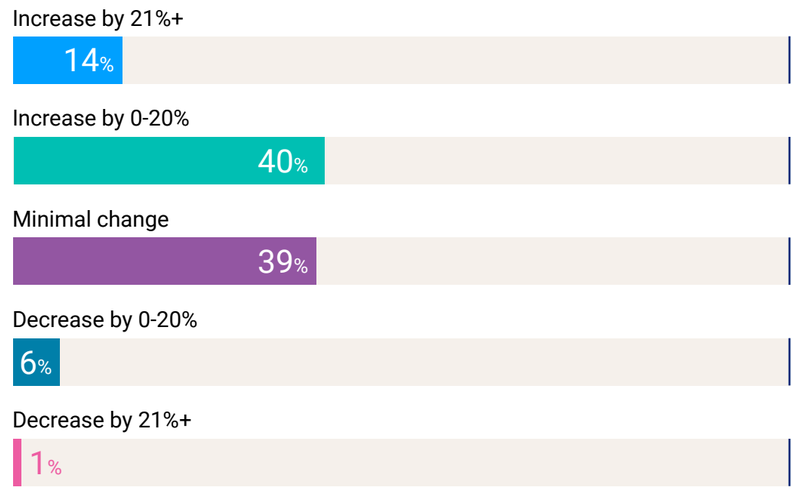
One of the reasons cited for this is the lack of available skilled workers in today's talent pool. In turn, those professionals are now able to command salaries which many employers cannot meet (another common factor among our respondents). In fact, almost half of employers in 2023 froze salaries for either existing or new members of their security workforce, while just 17% of respondents were able to offer a pay rise above 10% during this time period.

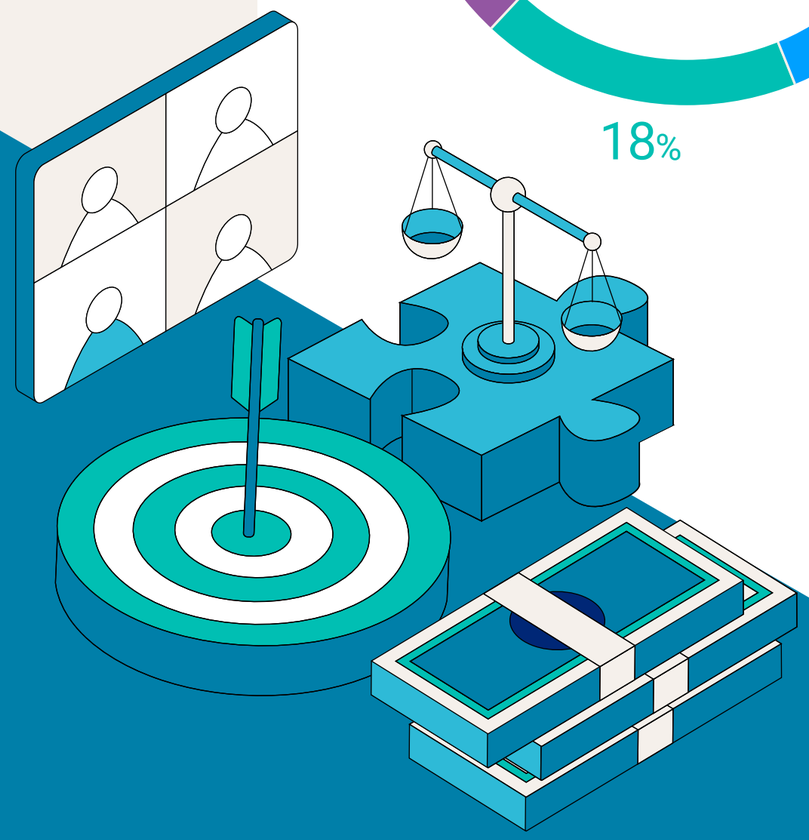
Moreover, this lack of investment in cyber security talent and teams sets a dangerous precedent. Of those surveyed, a greater proportion of leaders are significantly concerned about their budget compared to those surveyed for last year's report (72% in 2024, up from 68% last year). This is despite 54% of this year's respondents expecting an increase in their spending allocation (up from 46% in our 2023 survey). As such, attracting and retaining skilled cyber security professionals through monetary benefits is likely to prove more difficult, making alternatives, such as the development of non-traditional talent, more viable for employers in 2024.

Almost half of employers freeze salaries in 2023



Cyber security leaders forecast budget increase



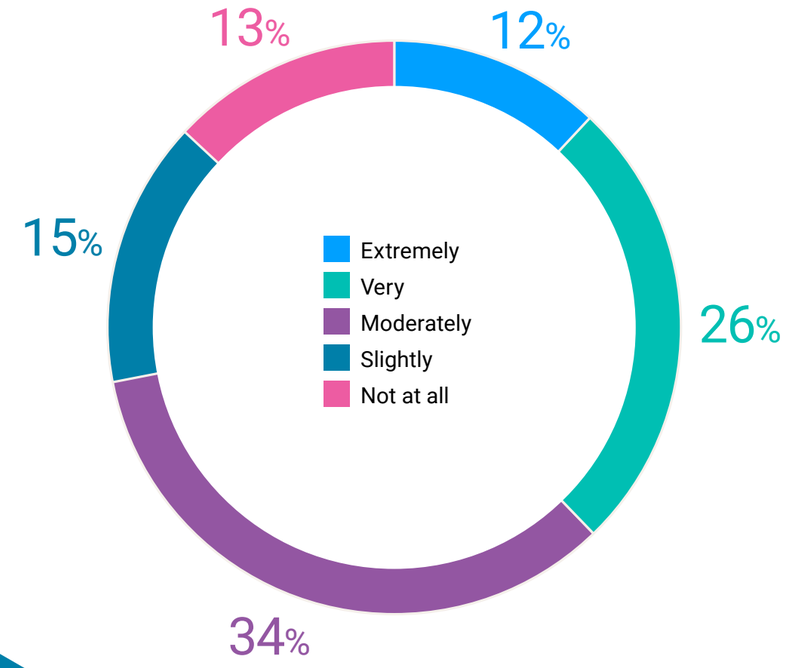


61%

do not rate their ability to attract cyber security talent highly

Concerns over budgets despite increase

To what extent are you concerned about your cyber budget in 2024?



Matthew Cotton
Head of Cyber Security Solutions, Hays ANZ

Our report has continued to highlight the challenges many cyber leaders face in hiring skilled talent. Finding candidates with the right skills and experience within budget is a constant challenge for many cyber leaders. Cyber roles continue to be more resilient and in higher demand than the wider tech space and, as we continue to see regular high-profile breaches, businesses are set to continue to invest in cyber programmes. As a shortage of skilled talent remains high, so do salary levels, creating a challenging environment for cyber leaders. This is also impacting the level of 'burnout' which is still a significant issue in the cyber area.

Businesses need to consider alternative ways to build their human capital capability in cyber. Utilising and upskilling from different areas of technology, and even outside ICT, should be part of the focus for many. Businesses should reconsider how they run their recruitment programmes to remove bias and create a level playing field that helps source talent from a wider pool, as well as invest in the next generation of talent. As universities continue to invest in cyber education programmes, more and more bright talent is being created that, with the right support, nurturing and mentorship, can become the next generation of cyber defenders that we all need to fight cybercrime!

Christian Toon
Head of Cyber Services, Pinsent Masons

Identifying and attracting cyber talent needs a specific solution, which can be difficult if it involves challenging the status quo within your organisation. For example, cyber security individuals are looking for greater flexibility but, when you're a small cog in a much larger machine that works typical hours, how do you go about changing one person's contract? The hirers may know what they need to do, but actually are confined by restrictions.

Think outside the box as to how you can offer something attractive within the confines of the organisational structure. What else can you provide, such as progression opportunities? Attitudes need to change because we're not hiring for life now. The workforce moves quickly, and you and your teams have to be prepared. Adopt the mindset of developing a production line of talent within your team.

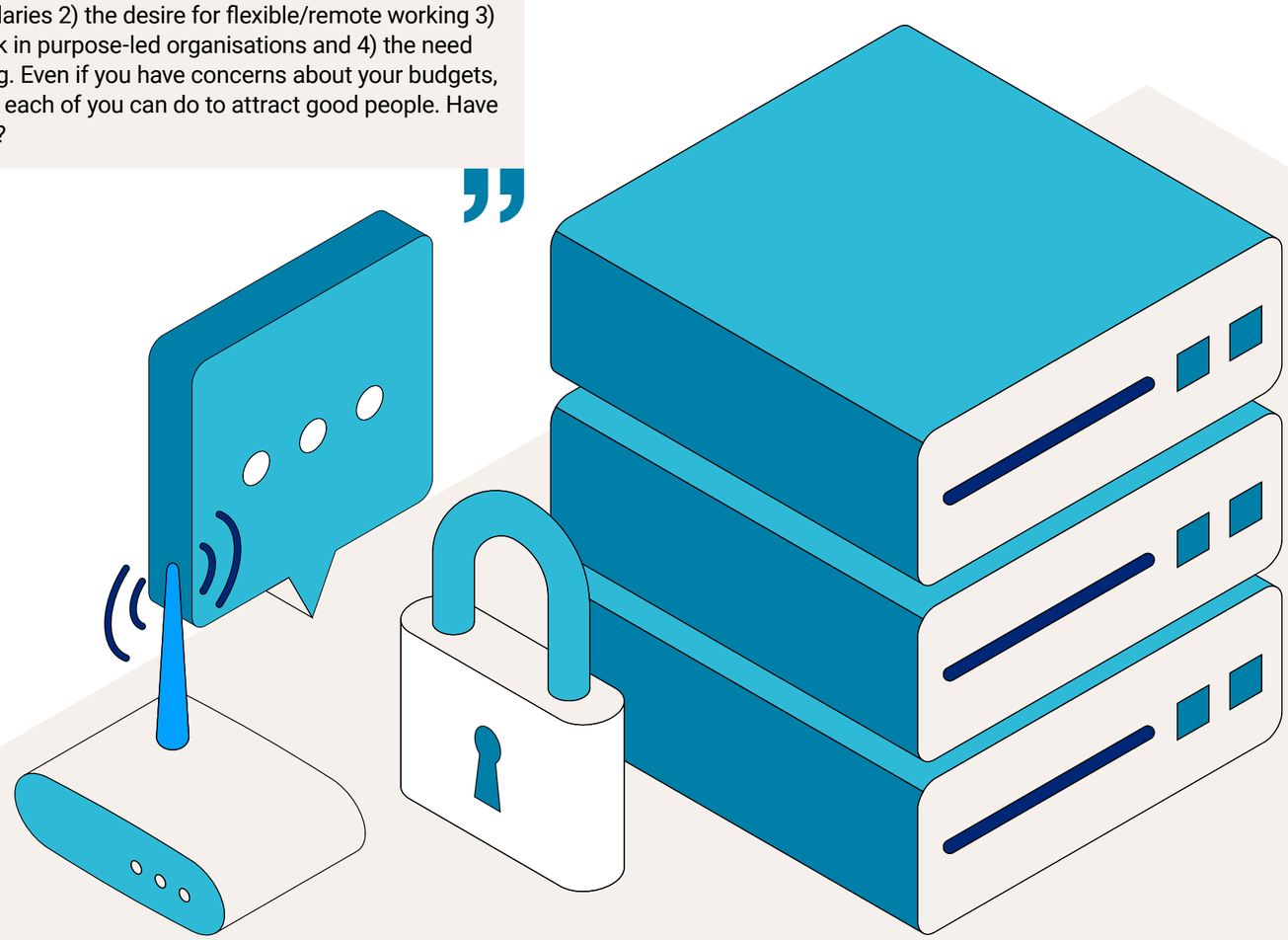
Sybil VR Kleinmichel
Cyber Security Managing Expert, Hays DACH

As a former Group CISO at a global bank, I am familiar with the "Cyber Skills Conundrum". This is the dilemma that many leaders in cyber live with today: global geopolitical and other risks drive business spending. This leads to hiring freezes, budget cuts or both in many industries.

I believe we are in a time of the most radical technological changes in history, combined with significant increases in cyberattacks. This leads to a high demand for jobs in cyber and gives candidates real career perspectives. For the providers of financial services and critical infrastructure in Europe, additional and new regulatory requirements add to the complexity. Ensuring effective governance, compliance and cyber security are both global and local concerns. To manage these risks, you must attract and keep good people.

Many respondents are doubtful of their ability to attract great talent. You can, by offering your people a great place to work, and by being the best leaders you can be. Our report raises four main employee priorities: 1) higher salaries 2) the desire for flexible/remote working 3) the preference to work in purpose-led organisations and 4) the need for continual upskilling. Even if you have concerns about your budgets, there are many things each of you can do to attract good people. Have you considered these?

For the providers of financial services and critical infrastructure in Europe, additional and new regulatory requirements add to the complexity.



CONSIDERATIONS FOR CYBER SECURITY LEADERS

TALENT **DEVELOPMENT**

With the recruitment of existing skilled cyber professionals proving a challenge for many respondents, training and development provides employers with an alternative talent source.

Of the employers who indicated that they are struggling to attract cyber security talent, 61% cite the lack of skilled candidates as a major factor. Given that experienced cyber security experts are at a premium, a viable alternative is the recruitment or reskilling of potential talent who demonstrate the transferable skills needed for success in a security role. This is a viable solution that can also support organisations struggling to offer competitive salaries to those existing skilled candidates.

Among our respondents, graduate pools and existing employees within the organisation were named as the main sources for their future cyber security workforce. However, organisations may be either unwilling or unable to commit to training or reskilling personnel from such backgrounds. One key finding of our survey is that 62% of respondents stated that their employer doesn't currently have an in-house talent development program to grow their cyber security workforce. As it stands, 73% of organisations invest 5% or less of their cyber security budget into developing talent. Meanwhile, almost twice as many respondents believed that any further investment should be dedicated to cyber headcount than into training resources.

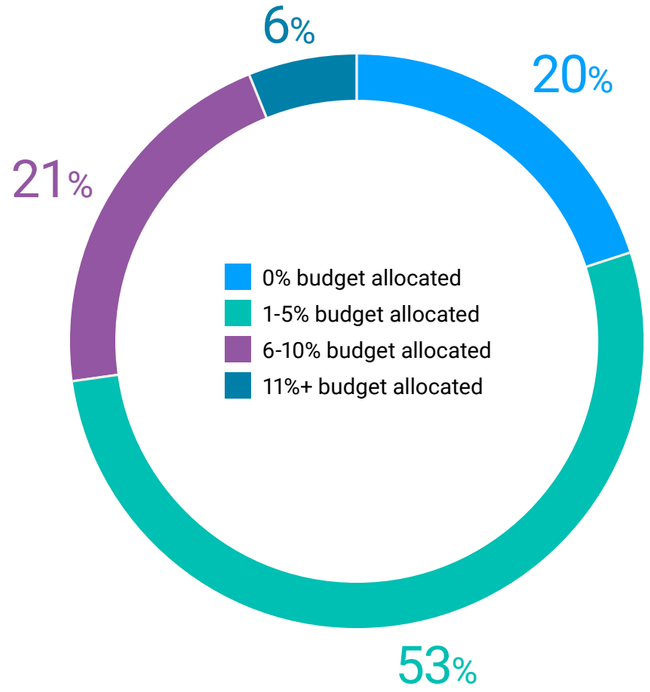
At present, it appears that organisations are failing to take responsibility for identifying and developing future talent, which is needed if companies are serious about retaining talent and filling their cyber skills gaps holistically. Without a higher prioritisation of this risk, combined with greater commitment from board members to focus and invest in this area, the challenge of building a better cyber security workforce is unlikely to either be successful or sustainable.

62%

of organisations
don't have a talent development programme

Low investment in talent development

What percentage of your cyber security budget is allocated toward talent development?



Most popular sources of future talent

1. Graduates
2. Internal
3. University
4. Other
5. Non-cyber disciplines

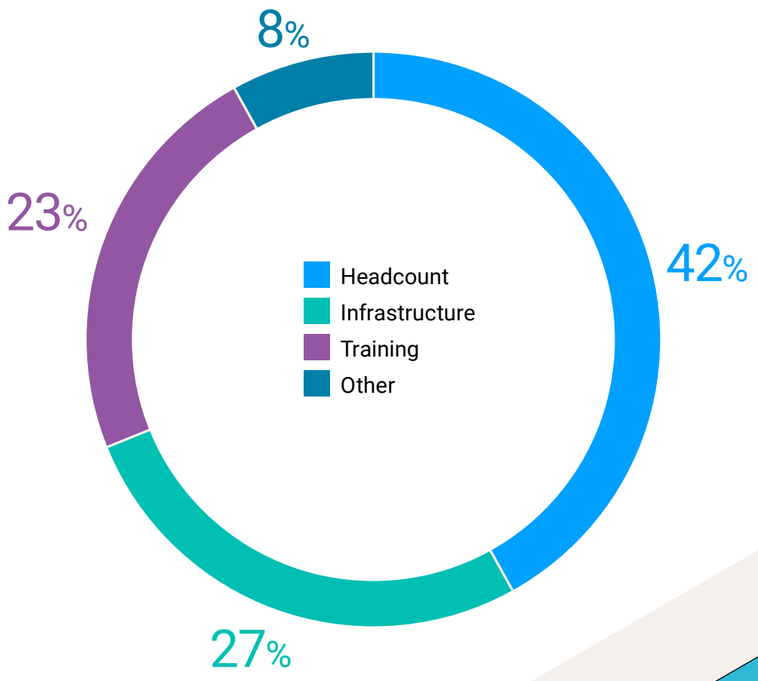
Given that experienced cyber security experts are at a premium, a viable alternative is the recruitment or reskilling of potential talent that demonstrate the transferable skills

Most shared challenges in hiring talent

1. Salary expectations
2. Shortage of skilled candidates
3. Lack of in-depth knowledge
4. Lack of experience
5. Competition from other companies

Leaders seek increase in headcount

In which area do you feel extra investment is most needed?



James Walsh

Head of Cyber Security Solutions, Hays UK&I

This year's report has highlighted the scarcity of 'ready-made' cyber talent globally. There is no immediate remedy for this challenging scenario, but there are certainly approaches organisations can take to mitigate and shift this paradigm.

One sustainable solution starts with cyber departments and their respective organisations making a shift from viewing themselves as simply 'cyber talent consumers' towards being 'cyber talent creators'. This can be achieved by leveraging the many training schemes out there to employ and deploy talent both from within and outside of their organisation. However, success depends on buy-in from Senior Leadership and HR/Talent departments, with input from the Cyber/Tech teams.

Throughout my years working in this sector, I can safely say there is no shortage of desire to work and upskill in cyber security. The challenge, instead, is overcoming the constant perceived requirement for 'ready-made' talent.

Neil Khatod

Head of Cyber Security Solutions, Hays Americas

As I joined Hays, I reflected on applying a few key concepts I learned in the military: as a soldier, we are taught to never accept defeat, nor leave a fallen comrade. This may seem ethereal, but applying these ideas to the cyber fight may mean the difference between a team's success and succumbing to the criminals. It is that determination and teamwork that says we must defend, we must win, and we must find a way to adapt as a team.

Building this workforce doesn't just happen. Employers need to look for adaptive, committed life-long learners who have a knack for solving technical problems. Often overlooked, the amazing, committed professionals leaving the military can and have solved so many challenges in the cyber domain. I've been privileged to watch these military cyber professionals in action, and I can speak firsthand to the benefits and talent level of bringing them onto a team!

As criminals constantly adapt, our defensive workforce must do likewise. It's up to us leaders to encourage a cadre of life-long learners.

One sustainable solution starts with cyber departments and their respective organisations making a shift from viewing themselves as simply 'cyber talent consumers' towards being 'cyber talent creators'.

ARTIFICIAL **INTELLIGENCE** & AUTOMATION

Artificial Intelligence's impact on the world of work both offers a solution and poses a challenge for cyber security teams worldwide.

While there is widespread belief among respondents (89%) that AI will prove useful in improving security capabilities, almost half of leaders believe that automation won't result in a loss of jobs, with only 36% predicting that it will do so by 2026. In the event of this forecasted impact, which suggests AI tools could be implemented to support professionals rather than replace them, upskilling and training on these technologies becomes an even greater priority.

Despite this, implementation is lagging behind. Only 57% of respondents will have trained their cyber security workforce on AI tools within the next year, with a quarter of leaders saying that they don't plan to at all.

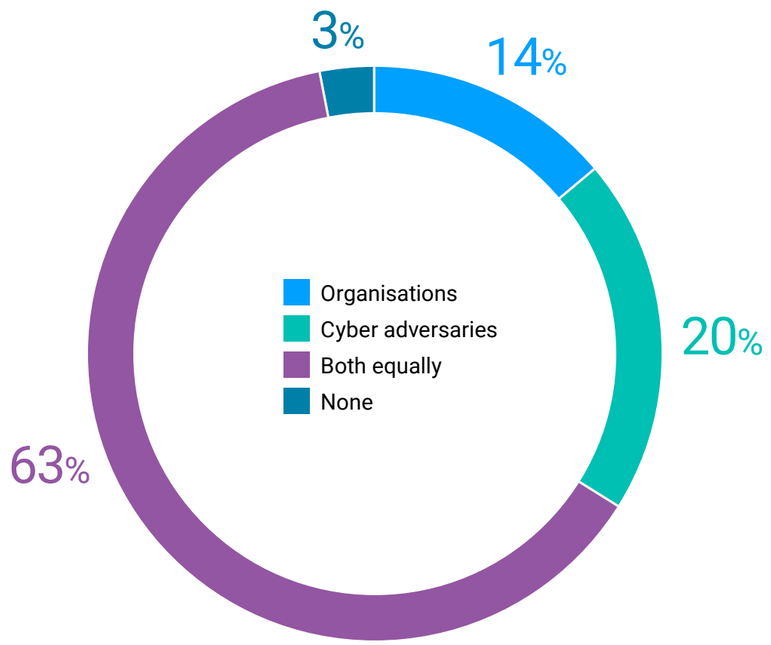
The European Union has released the draft regulation on the AI Act, which includes, among other things, requirements for high-risk AI systems. These will have to comply with a wide range of conditions, particularly related to risk management, testing, technical robustness, data training and data governance, transparency, human oversight, and cybersecurity (Articles 8 to 15). This means there is a real need for companies to ensure adequate AI competence and oversight. If 25% of the leaders who responded are not planning AI upskilling of their workforces, this status quo may represent a risk which is not yet being monitored adequately.

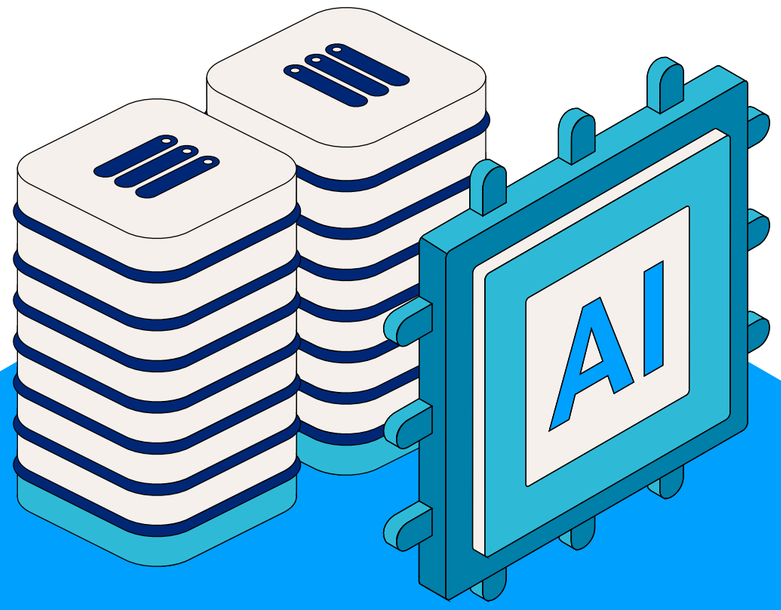
These attitudes come against a backdrop of significant concern over AI-based cyber attacks. While most respondents believed that this rapidly evolving technology will benefit both organisations and cyber criminals equally, there was a greater feeling that adversaries will gain the upper hand.

Failure to adopt these technologies, albeit in a safe and rigid framework, may leave organisations playing catch-up to attackers who are quicker to explore and utilise vulnerabilities. These are weaknesses created (as in the case of better phishing mails) or identified (as within publicly known vulnerabilities) with AI. Given that almost half of our respondents indicated that they are not planning on upskilling their workforce in this technology and the tools available in the immediate future, another troubling trend has been unveiled.

AI brings opportunities for all parties

Who will gain the biggest advantage from the evolution of AI?



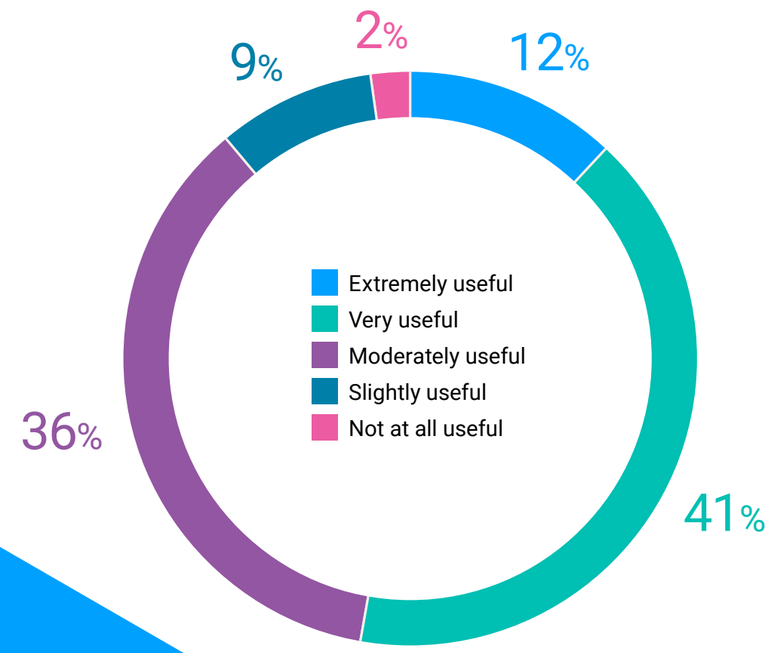


89%

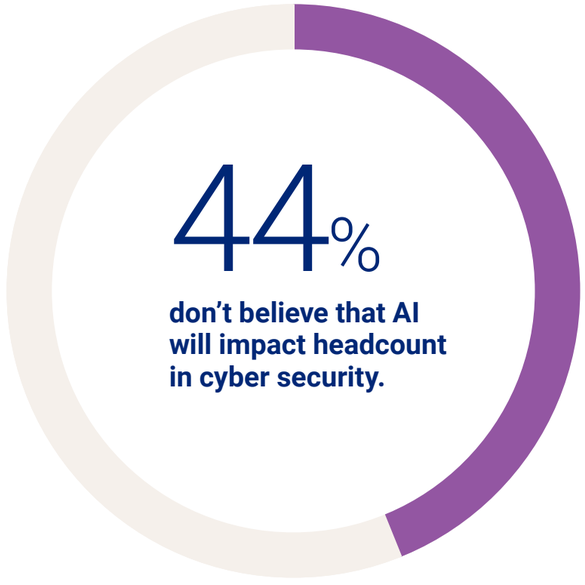
are **concerned** about the **potential risks of AI threats.**

AI has part to play in talent development

To what extent will AI prove useful for organisations in developing their cyber security team's capabilities?



Organisations split on whether AI can effectively replace cyber security talent



Julia Dudenko
CISO,
Haniel

"It's time to start exploring AI tools, but it must be framed as an exploration because we need to clearly explain the risks of using AI. When building an AI roadmap, it's important to find the balance between reaping the benefits while, at the same time, creating a robust framework to guide employees on what they can do with AI. If something isn't okay, what is the risk? Having an open dialogue about this helps to build understanding, which in turn makes it more straightforward to embrace the opportunities AI can bring.

On one hand, AI helps us to increase efficiency, so we might reduce the head count. At the same time, the AI used by criminals increases the number of attacks and their sophistication, so we might need more people to combat that."

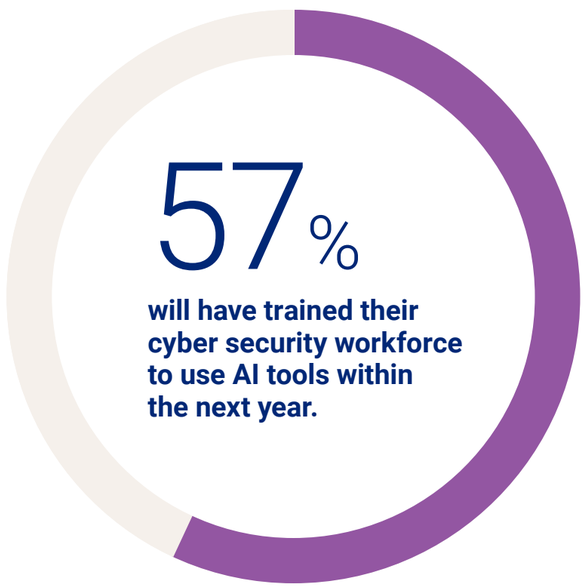
Jason Yuen
Partner, Technology Consulting and Malaysia Cybersecurity Leader EY

"There is such a shortage of professionals in cyber security that I don't think AI will affect jobs in the short to medium term. We just don't have enough people in the first place!

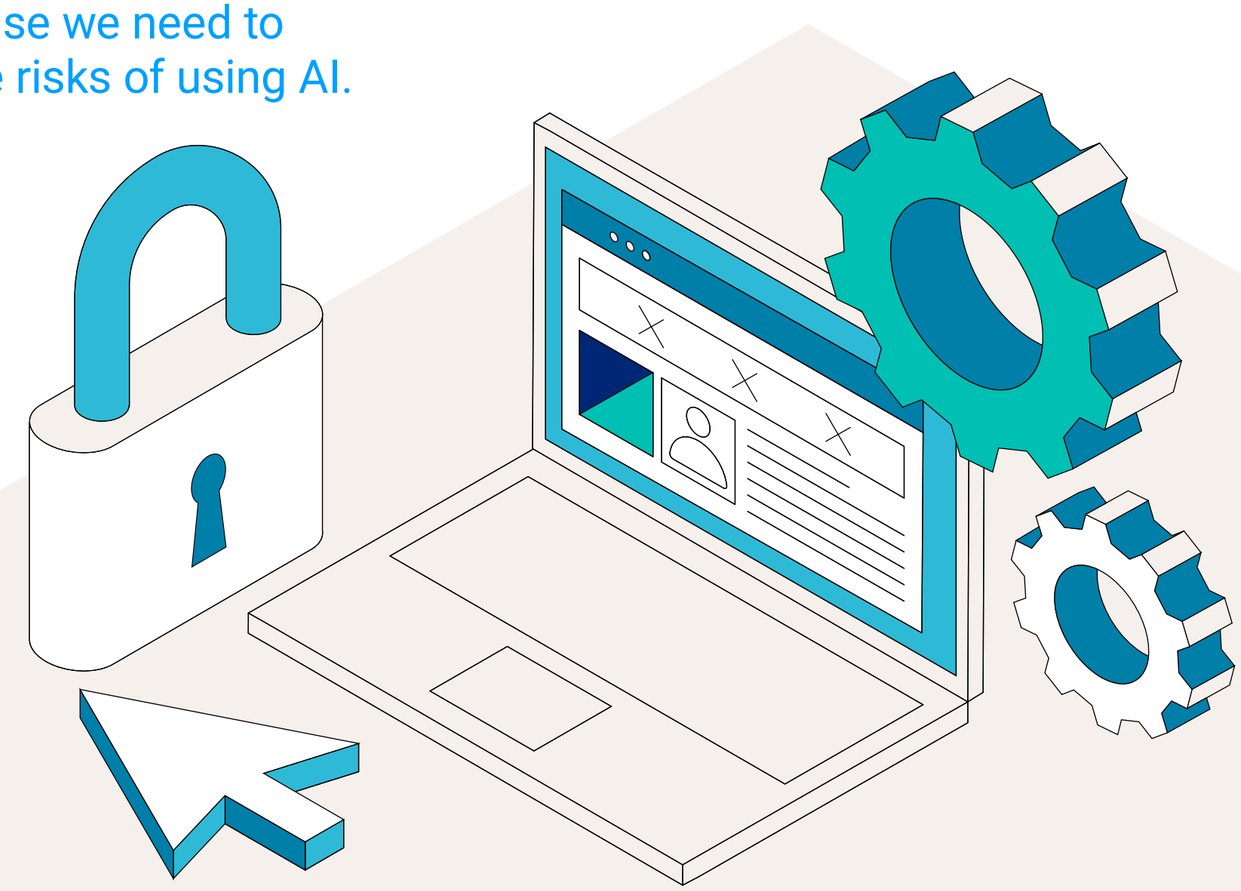
Where I see AI supporting us is speed of analysis. For example, what is it within my infrastructure that needs fixing? Where are my weak points? Where would criminals most likely attack? And I think the speed at which AI can match, for example, the types of attacks versus those my organisation is potentially susceptible to, is really useful. Traditionally, collating this information would either be too time-consuming or just not be worth the effort.

This is also where I see cyber security professionals providing value: being able to ask these questions and direct resources to where the remediation needs to happen in a more efficient way."

Organisations turn to AI for security



It's time to start exploring AI tools, but it must be framed as an exploration because we need to clearly explain the risks of using AI.



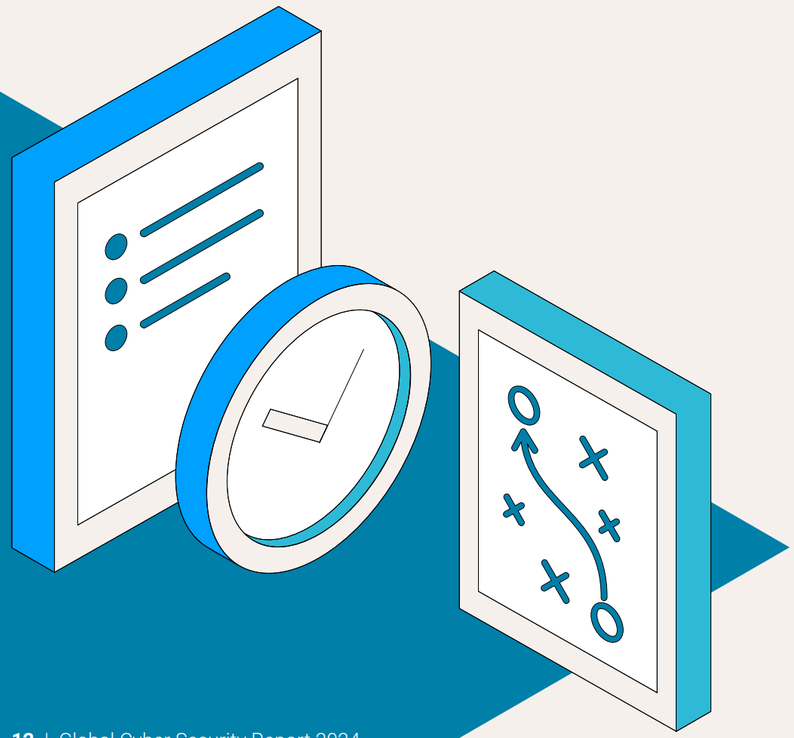
ACTION PLAN

This report has highlighted the extent to which cyber security leaders worldwide are struggling to bring in the skilled talent needed to protect and defend organisations in today's rapidly changing world.

Global economic factors continue to limit the investment that organisations are willing or able to make in security, further impacting opportunities to increase headcount or to pay competitive salaries in today's job market, where skills are at a premium.

Exploring non-traditional talent sources and internal recruiting methods can enable your organisation to close this cyber skills gap effectively, with a lighter strain on investment. Based on the results of this survey, many employers aren't considering meaningful alternatives nor providing access to the right kinds of training or opportunities for reskilling. This is a critical situation which we believe is set to worsen as AI technologies and skillsets rapidly evolve.

If your organisation is facing the same challenges that many of our respondents are experiencing, we have several recommendations for you.



1. Look at non-traditional talent

By considering people with transferable skills who may lack experience but are willing to develop, for roles within your cyber security workforce, your organisation can still find good solutions. To do this effectively, we recommend broadening your search to candidates with skills in wider IT and other disciplines, particularly those in administration and developer roles. At Hays, we've supported clients across the globe in identifying and assessing the right candidates to make the switch to cyber security. We also provide Cyber Advisory Services, which include one of our qualified experts (former CISOs, CIOs and COOs) assessing your current situation before designing a Cyber Skills Roadmap. This is customised to your current IT and cyber security compliance situation and information security strategy.

2. Devise training strategy to ensure sustainable success

Regardless of your cyber workforce's level of experience, continuous upskilling is required to ensure sustainable security. Employers cited training opportunities as among the best measures to attract talent and retain existing staff. If you're currently unable to offer a development plan for all, devising a Cyber Upskilling Training Strategy in your organisation can help you ensure that you're able to benefit by employing non-traditional cyber talent.

3. Embrace emerging technologies and ensure team are educated on benefits and pitfalls

Organisations must adapt quickly to a world in which AI solutions are becoming increasingly sophisticated, and at a rate we haven't previously witnessed. While the extent to which skilled workers can use these tools has yet to be determined, our study shows that respondents strongly believe that AI can support their team's capabilities. For organisations to fully take advantage of this, these tools must be incorporated into the security workforce's training and development.

Cyber leaders must collaborate with other departments (Data, Legal, Compliance, Internal Audit) and with Board Members to design and approve your company's AI Policy. Experience shows that internal rules in the form of a binding framework for using AI tools, including for defending against cyber adversaries (who can utilise them without considerations toward compliance or legality), is essential today.

4. Explore bringing contractors or Hays Cyber Advisors on board

While a permanent workforce might exceed your organisation's budget, recruiting "contract professionals" on an ad-hoc basis can be an affordable and adequate solution to filling your cyber skills gap today. Trends point to employers increasing their demand for technical contractors in 2024, something that Hays supports clients with regularly.

If your organisation requires cyber operations services, in the short term or on a part-time basis, it may be beneficial for you to consider changing your approach when hiring for roles such as Security Information and Event Management (SIEM) or Security Orchestration, automation and response (SOAR) Engineers, or Cyber Threat Intelligence consultants. Hays offers partnerships with vetted organisations which can provide these services on demand so that you can focus on your core business.

If you're unsure which approach is most desirable or effective, our Hays Cyber Advisors can help you with an "as-is/should-be" analysis, identifying quick wins and helping you to uplift strategic planning for all types of employment and external options for ensuring adequate cyber resourcing.

5. Ensure flexibility and remote working opportunities to attract and retain talent

Respondents listed opportunities to work remotely, the right work-life balance and greater flexibility as hugely popular benefits – both among potential cyber candidates and existing employees. If your organisation does not currently offer these to permanent and/or contracted staff, it's likely that you'll find it harder to hire and retain good cyber talent in 2024.

REGIONAL **INSIGHTS**

While this report has highlighted global trends and challenges, there were examples from our study of certain countries deviating from the consensus. We've picked out some notable data points from countries with the most respondents that offer further insight.

Australia

- 65% have increased headcount in 2023, compared with 53% across the globe.
- Just 40% see an increase to their budget in 2024, compared with 54% globally.
- Despite this, only 58% of respondents are 'Extremely', 'Very' or 'Moderately' concerned about their budget (72% worldwide).

China

- 'Work-life balance/Wellness' is most frequently cited as a retention strategy, while 'Remote/Hybrid working' was the most popular globally.

France

- 'Monetary benefits' were cited as the number one method for attracting talent – this wasn't among the top five reasons globally.
- As such, just 31% of respondents said that they didn't offer a salary increase in 2023, compared to 44% worldwide.
- A third of respondents believe that AI will be of greater benefit to cyber adversaries, while only 5% say that it will give organisations the upper hand (these percentages are 20% and 14% respectively across the globe).
- Only 24% think that AI won't affect headcount, compared to 44% globally. In fact, 57% believe it will make an impact within two years, a significant increase on 36% worldwide.
- Roughly two-thirds of respondents (66%) claim their budget will increase in 2024, as opposed to 54% across the globe.
- Despite this, 86% are 'Extremely', 'Very' or 'Moderately' concerned about their budget, compared to 72% worldwide.
- 38% claim that over 5% of their cyber security budget is allocated to talent development, significantly higher than the percentage of respondents who spend that much globally (26%).

Germany

- 55% of respondents don't believe that AI will impact headcount (compared to 44% overall).

Japan

- 26% of respondents have reported an increase in headcount in 2023, compared to 53% globally.
- Only 23% rate their ability to attract talent as 'High' or 'Very High' (39% worldwide).
- However, 74% have not offered a pay increase in 2023, compared to 44% worldwide
- 97% are 'Extremely', 'Very' or 'Moderately' concerned about AI attacks, compared to 88% globally.
- Just 34% will have started training their workforce on AI tools within in the next year, compared to 57% worldwide. Likewise, 53% aren't planning to do so, over twice as many as the global response (25%).
- Respondents feel that extra investment in training is more important than in headcount.

Malaysia

- Employers who rate their ability to attract talent highly cite the offer of professional development and career growth, as well as monetary benefits. Globally, respondents believe that greater opportunities for flexibility and work-life balance are more attractive.
- In contrast with the global view, more respondents believe that AI will benefit organisations over cyber adversaries.
- However, 98% are 'Extremely', 'Very' or 'Moderately' concerned about AI attacks, compared to 88% globally.
- Only 20% are currently training their workforce on AI tools – the global proportion is 32%.
- Just 31% believe that AI won't impact headcount, compared to 44% worldwide.
- 72% expect their budget to increase next year, much higher than 54% overall.
- Despite this, 92% are 'Extremely', 'Very' or 'Moderately' concerned about their budget, compared to 72% worldwide.

Singapore

- Only 28% rate their ability to attract talent positively, compared to 39% worldwide.
- Just 11% aren't planning to train workers on AI tools, much lower than the 25% worldwide.
- Regarding headcount, only 21% predict that AI won't affect headcount, as opposed to 44% globally. 55% believe it will make an impact within two years, much higher than 36% worldwide.
- 89% are 'Extremely', 'Very' or 'Moderately' concerned about their budget, compared to 72% worldwide.

UK

- Three times as many respondents view AI as beneficial to cyber adversaries (27% - compared to 20% globally) over organisations (9% - compared to 14% globally).
- 61% of respondents 'Extremely', 'Very' or 'Moderately' concerned about their budget in 2024 – a marked drop from 72% worldwide.

USA

- Only 47% of respondents don't rate their ability to attract talent highly, as opposed to 61% worldwide.
- 47% of respondents have a talent development programme within their organisation, compared to just 38% globally.
- Only 77% of respondents are 'Extremely', 'Very' or 'Moderately' concerned about AI attacks, whereas the global figure is 88%.
- 42% are currently training the workforce to use AI tools, a significant increase on the 32% globally.
- Likewise, 60% of respondents don't believe that AI will impact headcount – the overall average is 44%.

ABOUT US

At Hays, we invest in lifelong partnerships that empower people and businesses to succeed. We know that in a fast-moving market like tech, it's even more important to provide organisations with quick access to top talent who will make a real difference. We've spent years nurturing an ecosystem of highly engaged and unique candidates, and will work with you to grow or scale your business using our unique expertise aligned to sectors and technologies. Our insights are powered by experience, intelligence and data, made possible by our investment in new technologies and systems.

A trusted partner to organisations across the globe, whether you need a professional or a whole new team, we can help you plan for tomorrow.

If you're interested in discussing the findings or recommendations outlined in our report, please reach out to your local Hays representative today. We'll be happy to discuss the right solutions for your organisation's needs.

Americas – Neil.Khatod@hays.com
Asia – Mohammad.Qasim@hays.com.my
Australia and New Zealand – Matthew.Cotton@hays.com.au
CEMEA – Michael.Beaupre@hays.de
UK and Ireland – James.Walsh1@hays.com

Find out more at expertsintechnology.hays.com

Experts in
Technology