HAYS Working for your tomorrow

TACKLING THE **CYBER SKILLS** GAP

Global Cyber Security Report 2023

Experts in Technology

CONTENTS

INTRODUCTION

THE DEMAND FOR CYBER SKILLS

While it was already becoming a necessity for the vast majority of organisations, recent events have meant that the rate of digital transformation has accelerated over the last three years. That means an increase in data management, while hybrid and remote working means that workers need secure access to their employers' servers. These changes have afforded threat actors greater opportunities to exploit organisations and infrastructure than ever before, as well as provided added motive.

All of this has meant that the demand for people with cyber security skills has increased. At Hays, we placed over 750 people into roles in 2022 as organisations sought the talent needed to implement their defence strategies. However, as this demand outweighs the supply of people with experience or accreditations in cyber security, it's not always straightforward to fill those roles.

Is this skills shortage affecting organisations significantly? And, if so, how?

This is why we've decided that it's the right time to create our first global report. Our study, carried out in the final months of 2022, aimed to explore how organisations around the world have adapted their cyber security strategy to tackle today's threats, as well as the challenges they've faced in doing so. By surveying security leaders from across several industries and seniority levels, we wanted to discover which factors were impacting their ability to hire and retain talent, and whether the level of investment from their organisation is meeting their needs.

The most revealing finding was the extent to which organisations have been impacted by the lack of qualified candidates in cyber security. Overall, 90 per cent of leaders said the skills gap had affected their ability to implement their cyber security strategy.

It's not been easy to address, either. Hiring talent is an issue, with roughly two thirds of leaders admitting that they do not rate their organisation's ability to recruit people working in cyber security highly. Finding incentives to retain and train your existing talent becomes even more important, especially as they receive offers from organisations facing the same problem. Providing learning resources is attractive to employees and, given the benefits it brings to an organisation's cyber security strategy, the investment is worth it.

Despite this, many of our respondents were concerned about the funds being allocated to cyber security within their organisation. Although companies have reacted to global events by putting more money into security, almost half of leaders expect minimal change to their budget in 2023.

Our study has shown that finding and hiring the right talent is a significant challenge for businesses globally, and that the lack of skills is affecting security. What's the solution?

> 90% of leaders said the **skills gap** had affected their ability to implement their cyber security strategy.

At Hays, we like to talk about undiscovered talent. On one hand, these might be people out there who don't have the exact experience that organisations are seeking, but would be a huge asset if they're open to training. On the other hand, undiscovered talent may also refer to those who aren't given the same opportunities as their peers in either education or the world of work, but can bring plenty to your organisation. In addition to people coming from a low socio-economic background, there are also those we aim to help through our **Focusing On Employment Inequity report**, such as those living with a disability or young people struggling to start on the career ladder.

In this report, you'll find insights on all of the challenges that cyber security leaders are facing in 2023, from protecting their organisation to retaining trained employees. If you are having similar experiences to our respondents, we've also suggested some steps that you can take to ensure sustainable cyber security success.

Lastly, I'd like to thank all of the respondents who took the time to complete our survey. Without your help, we would not be able to provide these insights.

James Milligan
Global Head of Technology Solutions, Hays

ABOUT THE **SURVEY**

We carried out our research across 29 countries, surveying over 1,000 cyber security leaders. The study explored how organisations are responding to recent global events, their investment in cyber security, their challenges in hiring and retaining staff, as well as the skills our respondents sought and how these were developed among the workforce.

When examining the data, we investigated whether there were any discrepancies from region to region, in order to provide local insights. However, our analysis revealed little to no variation - the findings in this report reflect what is happening around the globe, as leaders face the same challenges and turn to the same solutions.

UKI and EMEA

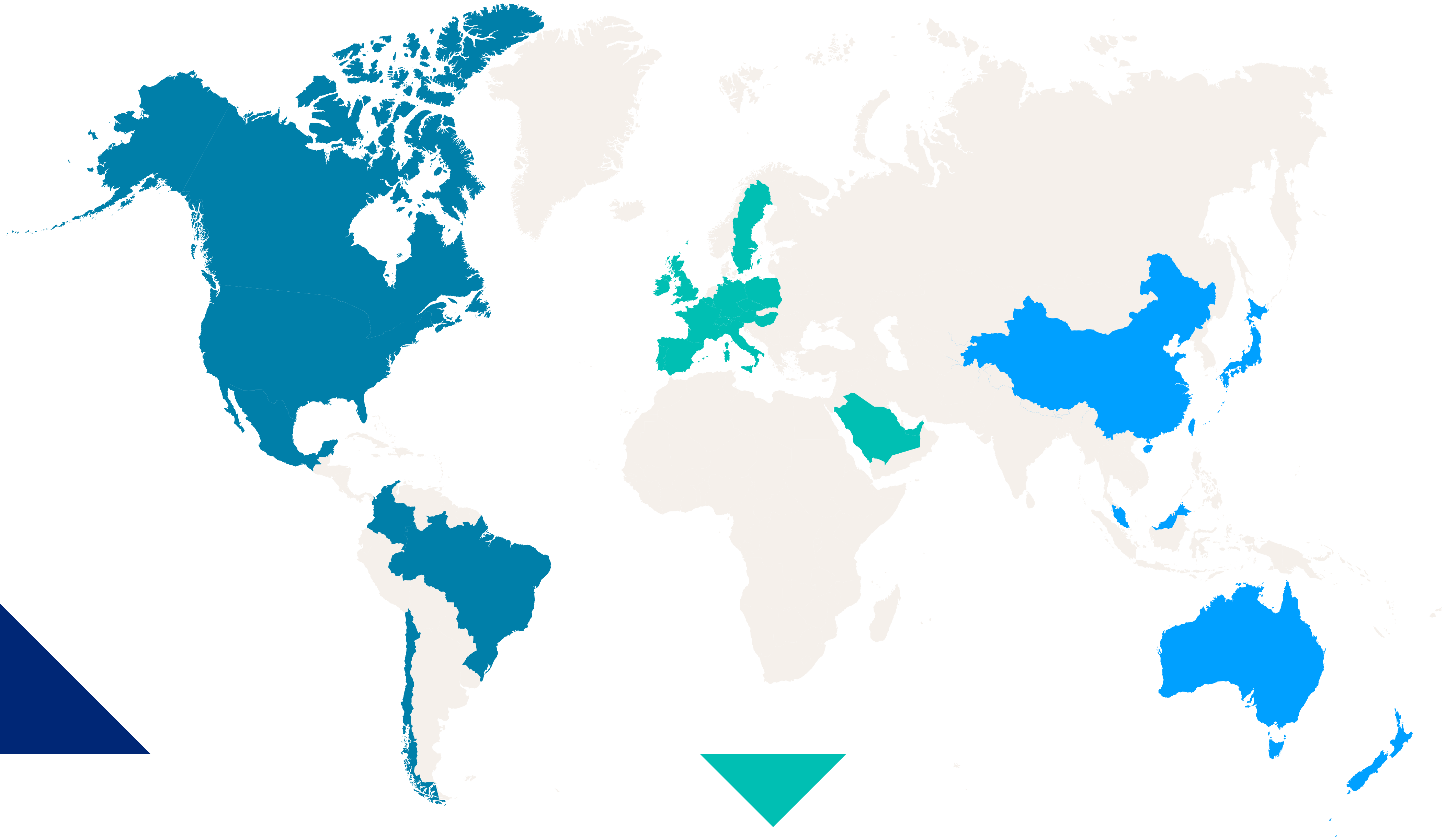
- Austria
- Belgium
- Czech Republic
- France
- Germany
- Hungary
- Ireland
- Italy
- Luxembourg
- Poland
- Portugal
- Saudi Arabia
- Spain
- Sweden
- Switzerland
- UK
- UAE

Americas

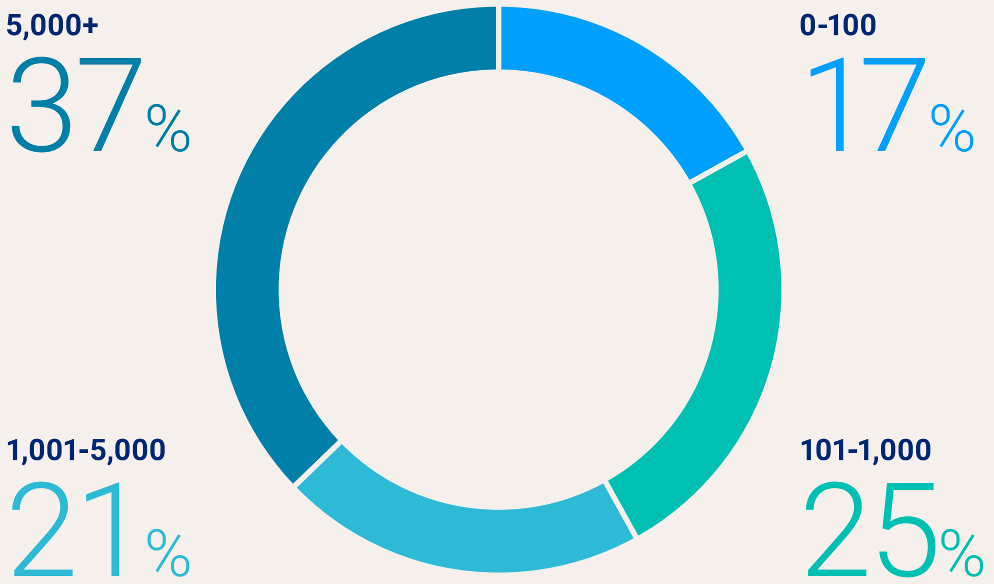
- Brazil
- Canada
- Chile
- Colombia
- Mexico
- USA

Asia and ANZ

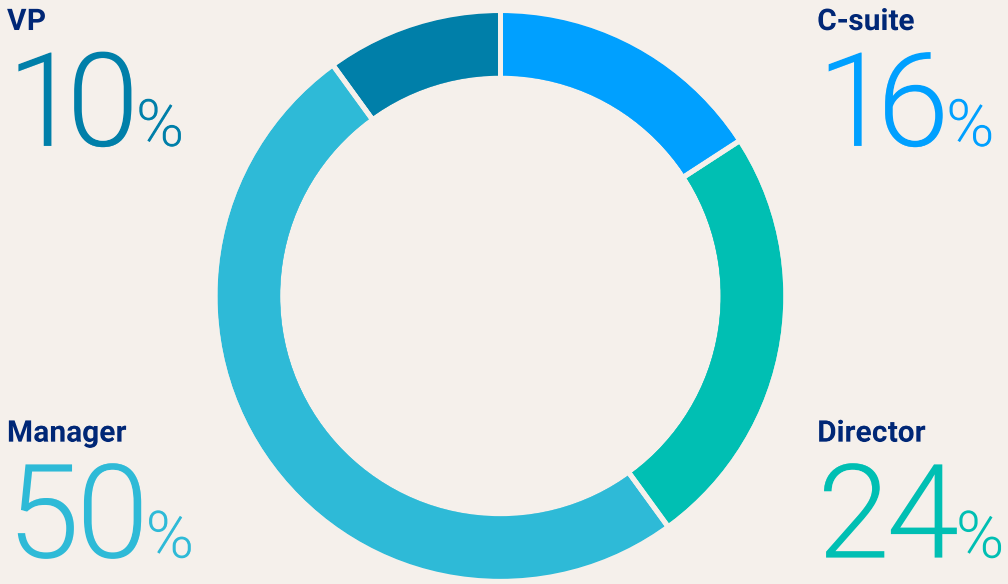
- Australia
- China
- Japan
- Malaysia
- New Zealand
- Singapore



Employees at our respondents' organisations



Seniority level of our respondents



ORGANISATION

In order to gain insights into how organisations are responding to cyber threats, we needed to understand how they are being affected and where their security team fits in the reporting line.

Many leaders report that recent global events, such as geo-political conflicts and the pandemic, have affected the cyber risk profile at their organisation.

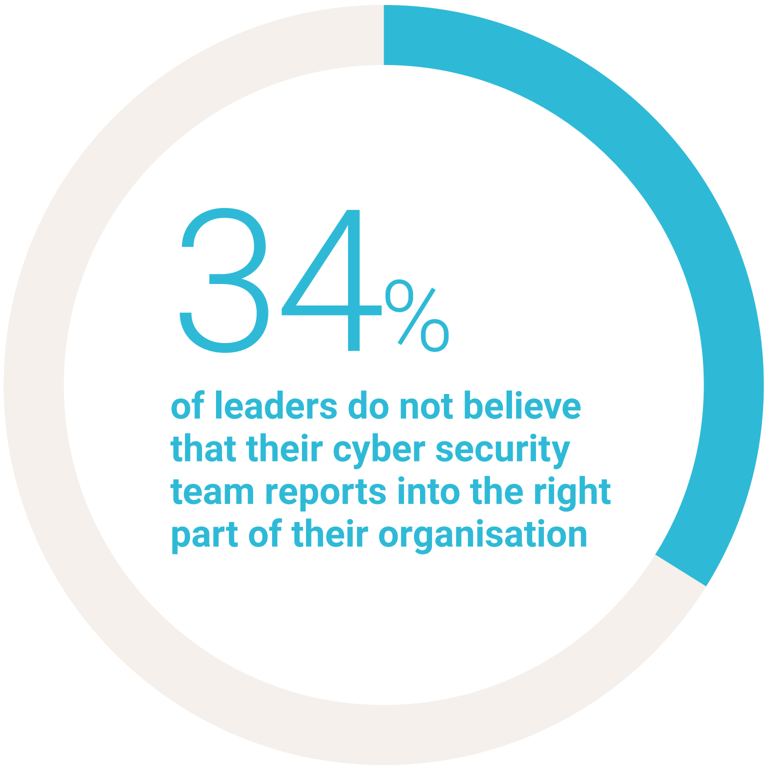
The pandemic in particular has accelerated the need for digital transformation, which has given greater opportunities to cyber criminals - 84 per cent of leaders reporting that their organisation experienced a phishing attack in 2022. Employees have had to become savvier as a result, with 77 per cent of leaders reporting that cyber security awareness is greater than it was three years ago.

Organisations have had to respond swiftly to combat potential threats, but incorporating cyber security into their strategy has not been a natural process for everyone. A third of leaders do not agree that cyber security sits in the correct reporting line within their business.

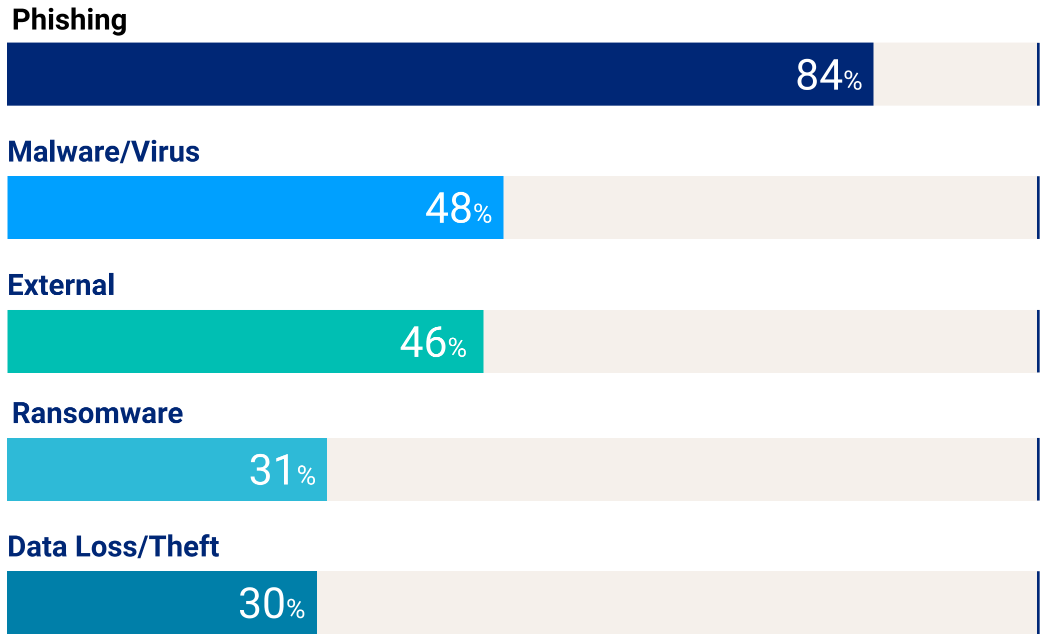
77%

of leaders state that **security awareness** in their organisation is greater than in 2019

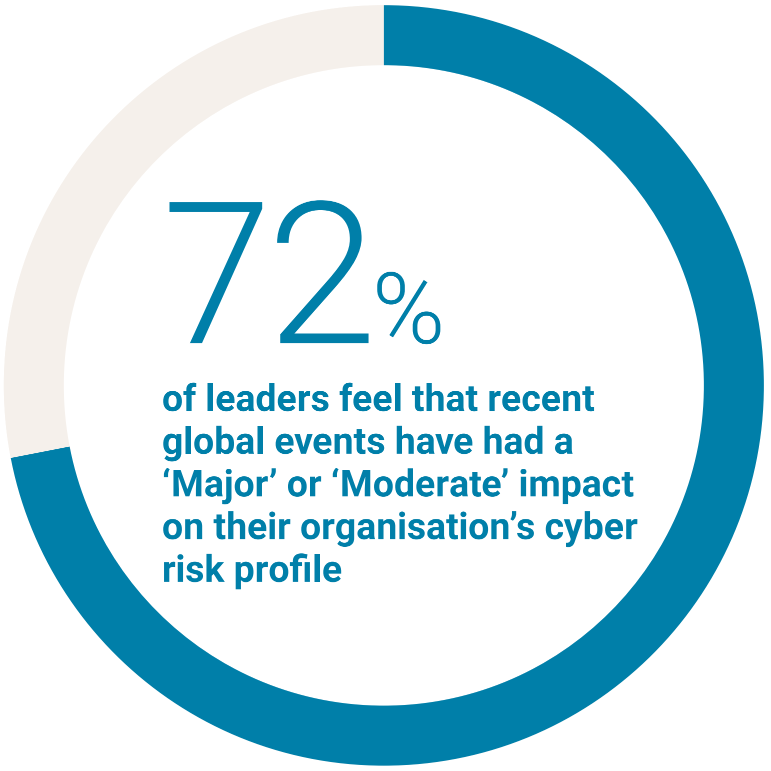
Cyber security teams are not always positioned strategically



What type of attacks have you experienced?



The pandemic and geo-political climate have affected organisations' security

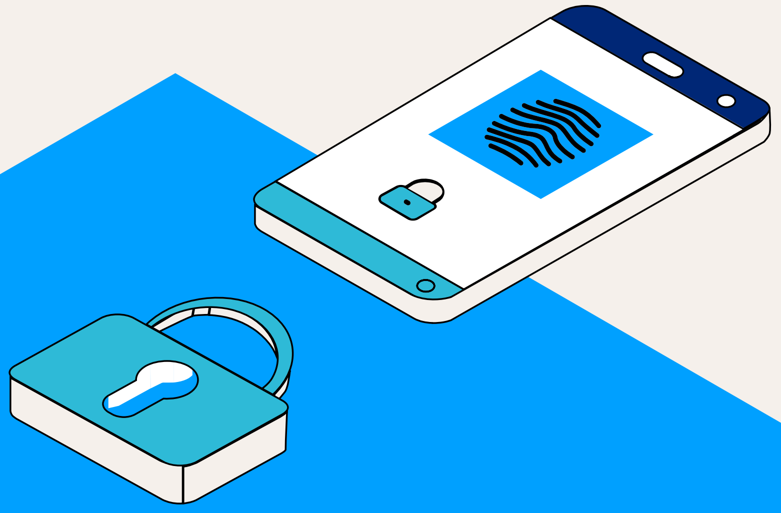


INVESTMENT

We wanted to explore how organisations are investing in cyber security, and whether their budget has increased as a result of global events and trends.

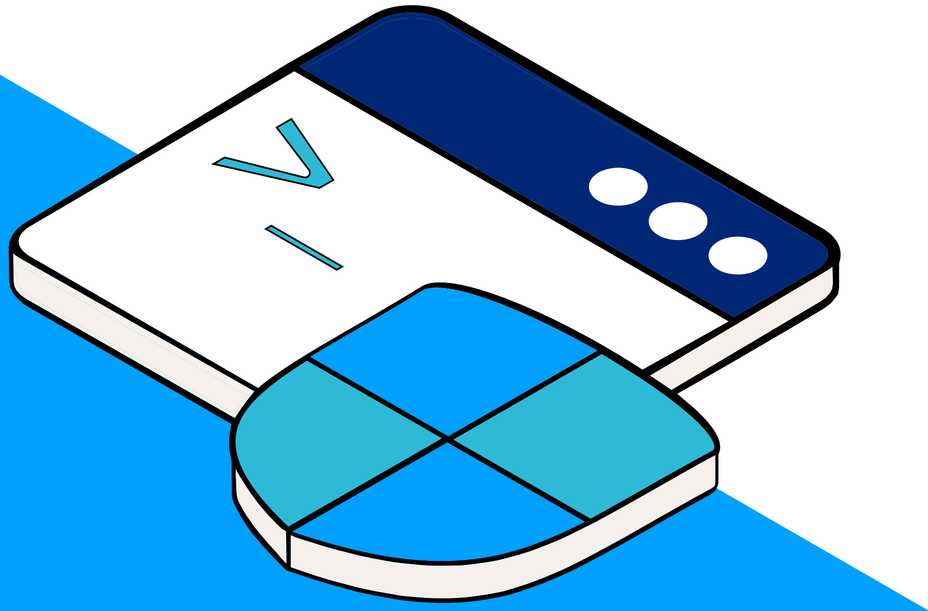
With security a concern across the globe, leaders are looking for a financial commitment from their organisation. Over a fifth of our respondents report that at least ten per cent of their organisation's IT spend is allocated to security.

However, while only 17 per cent of leaders disagree with the statement that investment in cyber security has been easier to receive since the pandemic, almost half expect minimal change to their budget in 2023. As a result, there is a concern over whether investment in cyber security will be sufficient for tackling today's threats.

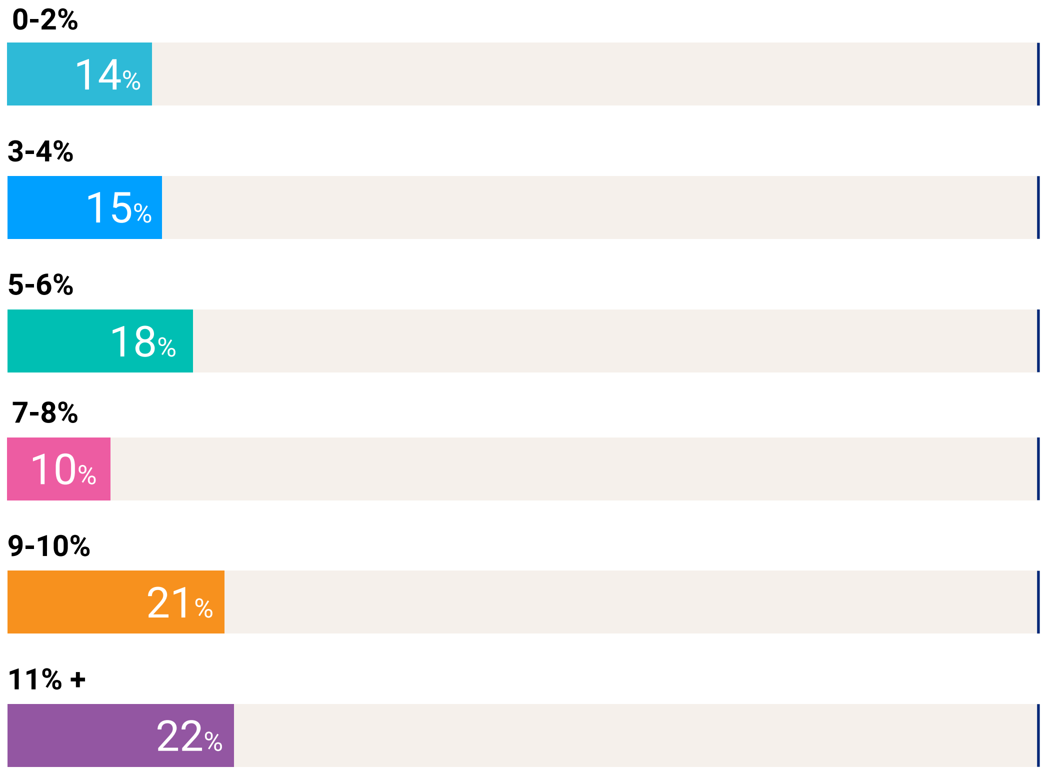


68%

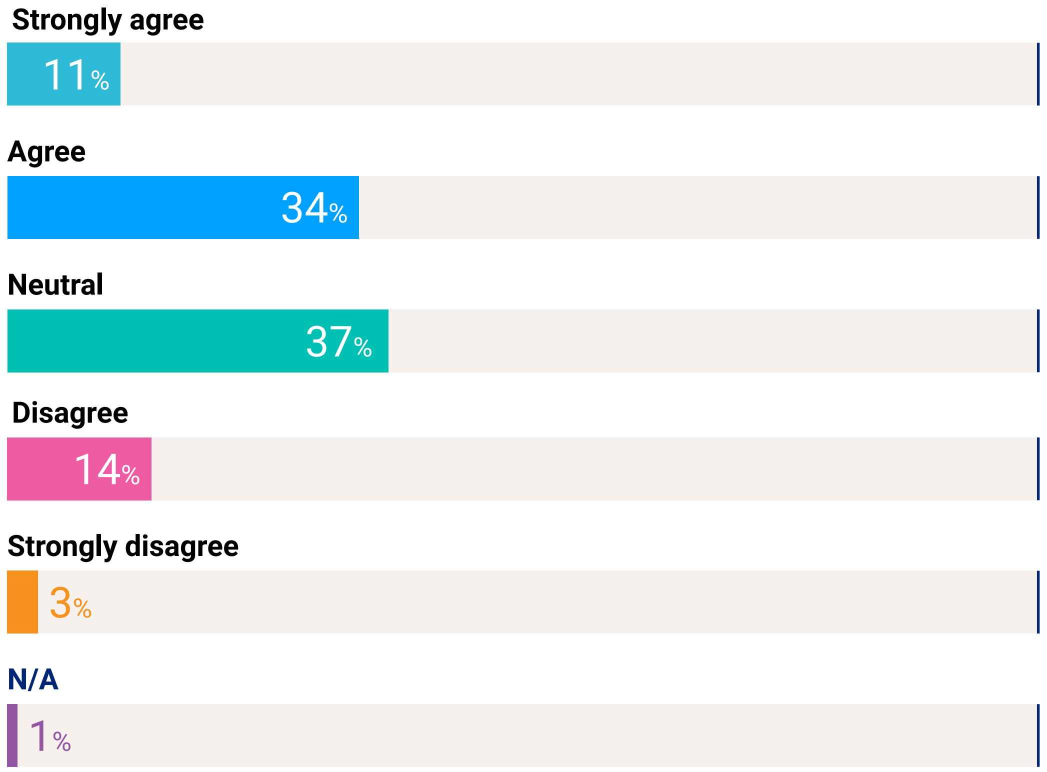
of leaders are "Extremely", "Very", or "Moderately" **concerned** about their budget in 2023



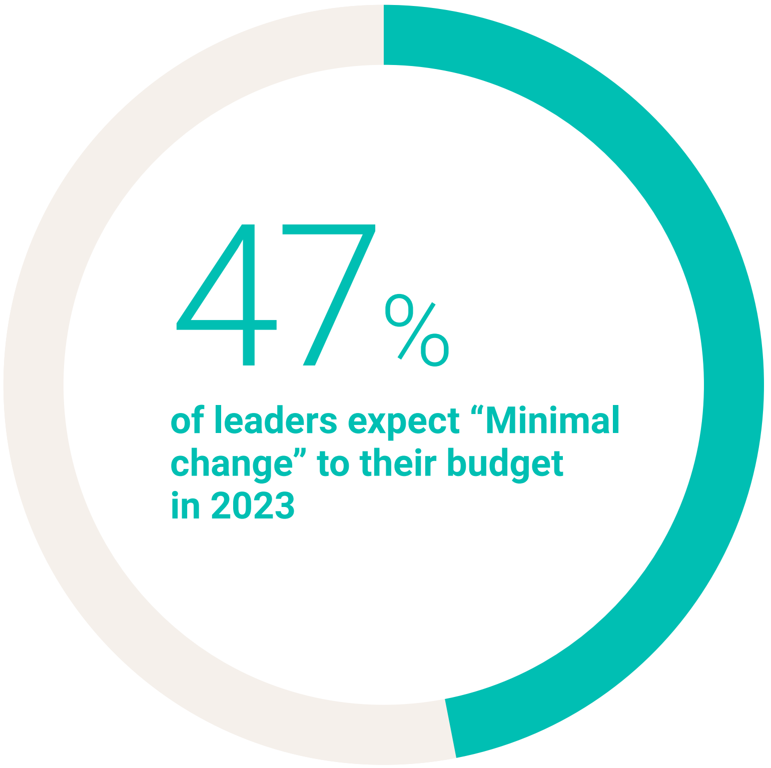
What is your organisation's annual spend in cyber security in proportion to IT budget?



Obtaining investment in cyber security has been easier since the pandemic



Investment is not necessarily aligned with security leaders' needs



47% of leaders expect "Minimal change" to their budget in 2023

HIRING

With the skills gap posing problems in tech, we wanted to understand the challenges that organisations face in recruiting talent.

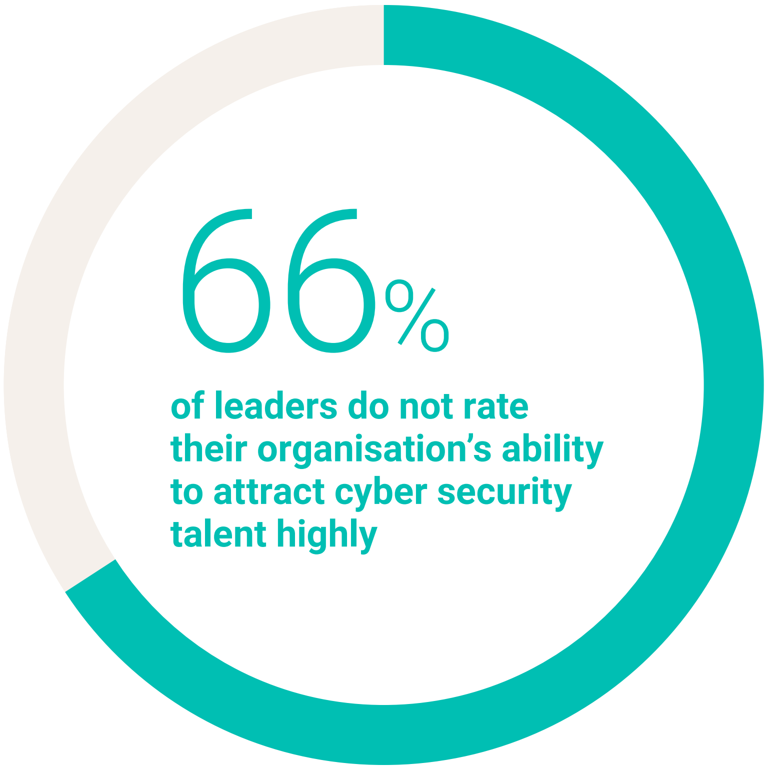
When asked what would improve the security capability at their organisation, leaders mostly named skills that would reinforce the front line of defence, such as cloud security and architecture. This aligns with our own insights, as globally we're seeing highest demand for engineers and architects. However, the challenge is to find workers with the knowledge and experience required to fill roles within their organisation.

Meanwhile, leaders face competition in hiring those with the right credentials, who, in turn, are able to demand a higher salary. In fact, two thirds of leaders do not rate their ability to attract cyber security talent highly.

This means that organisations must look for unexplored or untrained talent, an approach that they are open to. Over half of the leaders surveyed state that they are likely to hire workers who don't hold formal accreditations.

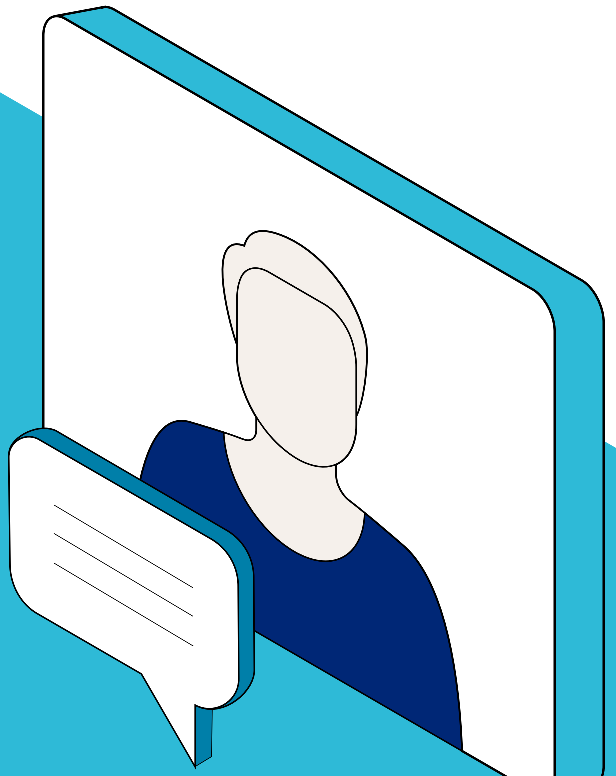
> "Two-thirds of leaders do not rate their **ability to attract** cyber security talent highly."

Organisations struggle to recruit cyber security talent



66%

of leaders do not rate their organisation's ability to attract cyber security talent highly



Organisations seek front-line skills

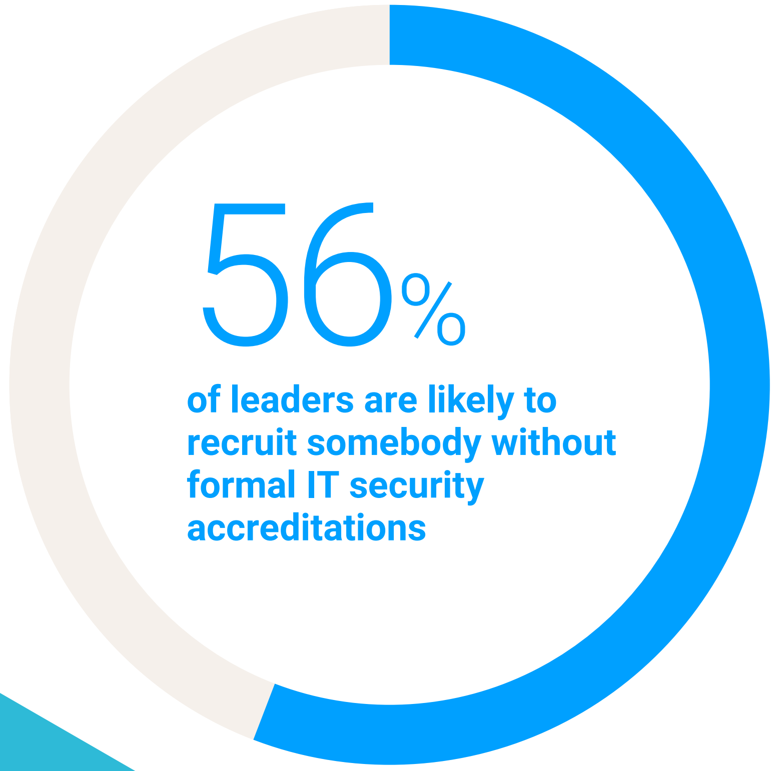
Top five challenges in hiring talent

1. Salary expectation
2. Missing skills
3. Competition
4. Length of working experience
5. Lack of experience at a similar organisation

Top five skills/implementations that would enhance security capability

1. Cloud security
2. Governance, Risk and Compliance
3. Security Architecture
4. Security Engineering
5. SIEM/SOC

Employers are turning to unexplored talent



56%

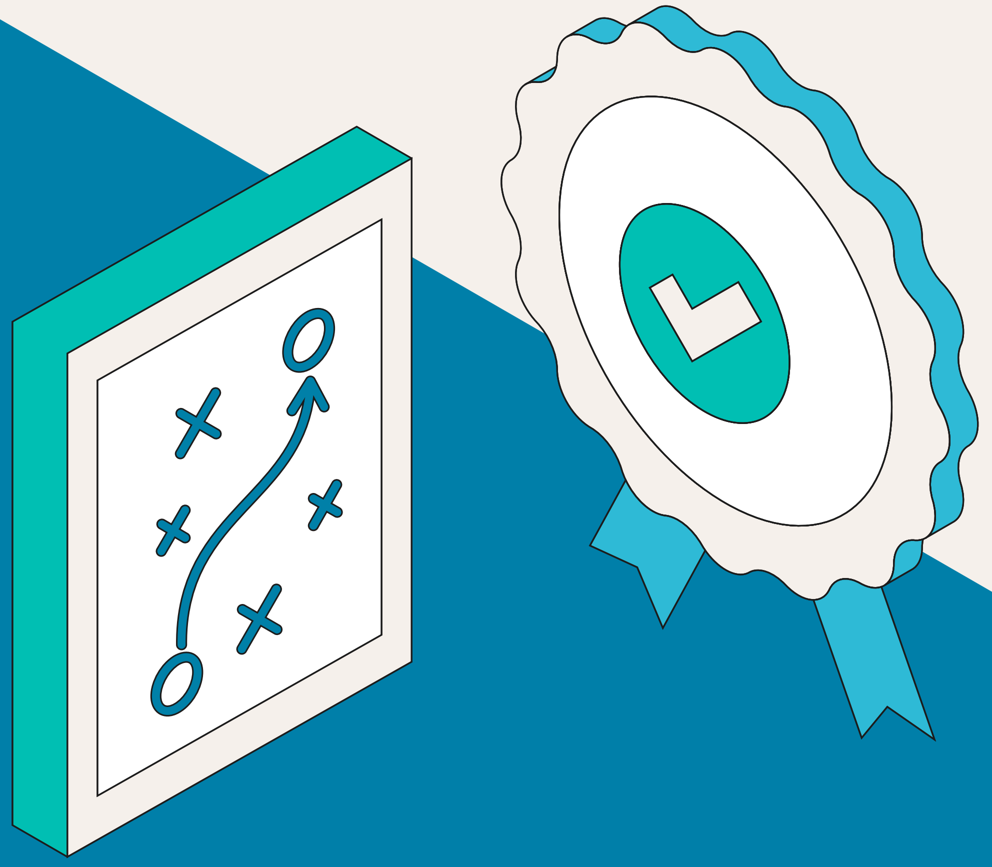
of leaders are likely to recruit somebody without formal IT security accreditations

RETENTION & SKILLS

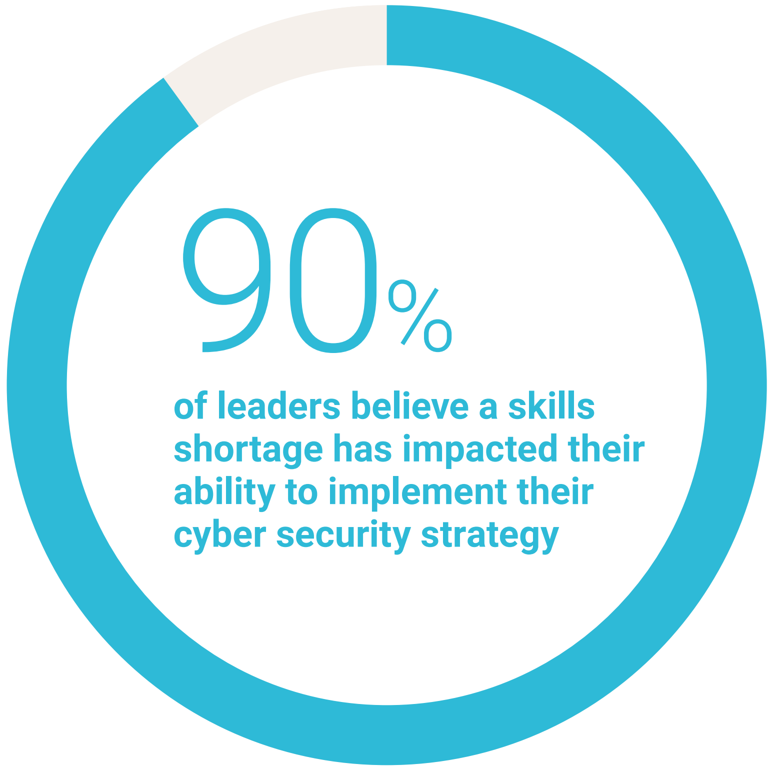
In addition to hiring, how are organisations retaining existing talent and equipping them with the skills they need?

The shortage in skills is having an impact across the board, with 90 per cent of leaders revealing that it has affected their security implementation. If the experienced talent isn't readily available, organisations must find new ways to fill these roles.

In order to close the skills gap, leaders believe upskilling and cross-training their team members (i.e. teaching them how to perform in new roles) are the best routes to success. Indeed, many leaders report that their organisation invests in training employees; however, this investment does not stretch to retaining their existing talent, as employers instead offer work-life balance perks over monetary reward.



Skills shortages are affecting security



90%

of leaders believe a skills shortage has impacted their ability to implement their cyber security strategy

> "Many leaders report that their organisation **invests in training** employees; however, this investment does not stretch to **retaining** their existing talent"

Skills development is used for the benefit of organisations and workers alike

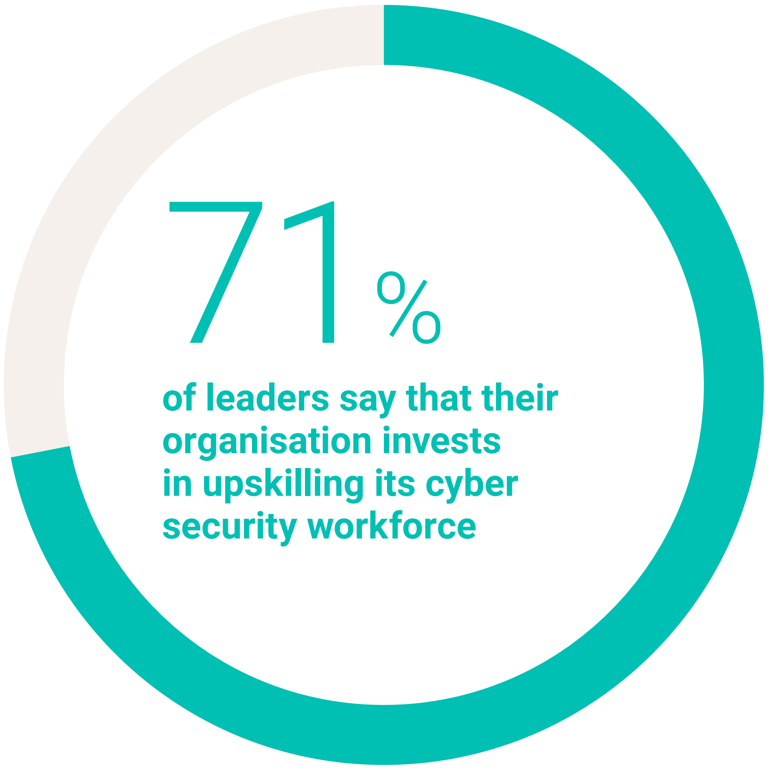
Top five strategies to close the cyber security skills gap

1. Upskilling
2. Cross-training
3. Recruitment partner
4. Hire, train and deploy
5. University outreach

Top five strategies for cyber security talent retention

1. Remote and hybrid working arrangements
2. Work-life balance / Wellness offering
3. Flexible hours
4. Professional development opportunities
5. Career growth & progression

It's necessary to equip the workforce with new skills



71%

of leaders say that their organisation invests in upskilling its cyber security workforce

THE HAYS **VIEW**

Hays experts give their thoughts on the findings in our report and what they mean for leaders in 2023.

Edmond Pang
Director, Cyber Security, APAC

Similar to the global landscape, there is no surprise that cyber threats have increased in the APAC region given COVID lockdowns being the perfect storm, with some high-profile breaches highlighted in the media. As a result, we're seeing countries stepping up with their policies and investment into cyber.

For example, Australia has increased penalties for businesses that do not sufficiently protect customer data, while the Security Of Critical Infrastructure Act (SOCI) has been amended to strengthen the security and resilience of critical infrastructure. New Zealand has updated and finalised the New Zealand Information Security Manual (NZISM) with four policy changes in September 2022. Japan has stepped up on regulatory requirements in industries such as Banking and Insurance, and the Malaysian government has announced increased fundings into the Tech & Cyber security space.

Overall, the APAC cyber market will continue to be hot but there are extreme challenges related to the constant war for talents. Apart from the typical security roles, we have seen an increased need for talents within GRC, CTi, IAM and Security Forensics across the region, but again a lack of suitable talents within the market.

James Walsh
Director, Cyber Security,
UK & Ireland

As across the rest of the globe, the cyber threat to UK&I organisations has been growing exponentially. There is a battle to combat a variety of threat actors across all sectors and, ever increasingly, a war for talent too.

As an industry, we have to look more at bringing in diverse talent pools that offer different skills and approaches to tackle the problems. A positive from the report is that over 70 per cent of organisations invest in upskilling their cyber professionals. Through our Permanent, Contract, Statement of Work and Hire Train Deploy offering, we are helping organisations to improve their security posture and diversity.

Miguel Duran
Director, Cyber Security,
North America

I am very excited for this inaugural release of the Hays Global Cyber Security Report. With the ever-growing demand in the market, we at Hays wanted to provide a comprehensive deep dive into the global and regional challenges security leaders face and how key global events have affected the threat landscape, along with how to adapt and overcome in a heightened skill-shortage economy.

This, along with our annual salary guide, will be a great tool for cyber leaders to use, and help overcome internal conversations around how to pivot in this fluid state we are currently in.

Michael Beaupre
Head of Cyber Security Solutions,
EMEA & DACH

Cyber crime tears through our lives like a raging storm and does not discriminate. It can devastate any company anywhere. From small local businesses to large global enterprises and everything in between.

Are we collectively prepared to weather these cyber storms? The majority of employers are struggling to hire top talent and see this gap as a significant risk to their cyber security strategies. We must partner as a community and develop new and innovative ways to attract, train, and retain cyber security talent.

Over two-thirds of security leaders polled around the world are worried about their budget, and we must jointly optimise our investments in cyber security technology and capability. This means working together with cyber security providers and talent providers on a broad scale and engaging board level leaders to identify the most critical assets in each company. We can't afford to protect everything, and we must prioritise based on risk, resiliency, and operational relevance.

Understanding that we are all in this fight together and the challenges we face are not unique to our countries or our industries helps us share solutions and capabilities across boundaries. Cyber criminals know no boundaries, and our responses should harmonise across borders.

> As an industry, we have to look more at bringing in diverse talent pools that offer different skills and approaches to tackle the problems.

CYBER IN THE SPOTLIGHT **VIDEO SERIES**

In our YouTube mini-series, we spoke to cyber security leaders worldwide to gain insights into the way they work, the changes they're seeing and the challenges they navigate.

LAB49

Deepayan Chanda

Principal Cybersecurity Architect, Lab49

With this constant skills shortage challenge, IT certifications or any kind of education in cyber security do play a valuable role. However, in order to get the most value out of certifications, people should align these with the career path they're choosing. I believe that most certifications are not dependent on location.

There are multiple things we can do to hire and retain talent. Let the candidate or employee know what the role is all about – there should be no ambiguity in the role definition. Keep an eye on market trends, as compensation does play a huge part in retaining talent on a case-by-case basis. Lastly, and possibly the most important: empower the role itself. People want to see the impact of the work they are doing and, if that is not visible, then it's really a challenge to keep talent.

Watch the full interview here ▸

fenergo

Niamh Muldoon

CISO, Fenergo

Attracting talent is one thing, retaining talent is something different. It's up to a CISO to retain top talent. It's about understanding where people want to go in their career and fuelling them with the skillset, expertise and experience to get there. People need to know the big picture and understand what they can get in terms of opportunities from their organisation.

We're very focused on technology. If you take a step back and look at what information is all about, it's confidentiality, integrity and availability of data. The opportunity there is to think about security in a wider context, and not just focus on technology.

Watch the full interview here ▸

MANDIANT

Ron Bushar

Senior VP and Global Government CTO, Mandiant

In the same way that there's a global arms race in cyber, there's a global talent race in the same dimension.

We've recognised that you can't continue to take the approach of, "I only want the best person in cyber intelligence, I only want the best incident response guy in the world etc." There's only a few of those, so we have to shift our thinking around how to train and equip the next generation.

Don't just look at somebody's resume and say, "they don't have 20 years of experience and a degree in cyber security, so they're no good". It is so important to embrace diversity, expand your aperture of who you're attracting to come to the organisation and then take the time to train them.

I can't tell you how many candidates come through that you would say don't have the traditional experience, but have been able to come into a role, train with experts in the field and quickly become extremely capable.

Watch the full interview here ▸

It is so important to embrace diversity, expand your aperture of who you're attracting to come to the organisation and then take the time to train them.

NEXT STEPS

This report has highlighted that the skills shortage in cyber security is having an impact on organisations' defence strategies. With this skills gap posing a problem for many cyber security leaders who are hiring, it's important that organisations find an effective solution. Here are some recommendations we have for next steps:

Consider unexplored talent

Although they may not have the experience or complete skillset, there are people out there with the learning mindset to help your business. Broaden your search and think about the relevant skills any recruits would need and which they could build upon with the right training.

Similarly, there's talent with the skills you're looking for, but who have so far found it difficult to get on in the world of work. Hays is partnered with neurodiversity experts Genius Within, who assist organisations in bringing in neurodivergent talent. We also focus on developing and training those who face barriers in getting into the workplace, such as people from lower socio-economic backgrounds or those living with a disability.

Upskill your current talent

It's vital that your organisation stays ahead of cyber criminals through continuous learning. Ensure that senior leadership are aware of its importance and that your cyber security team are familiar with the latest practices and technologies.

At Hays, we provide solutions and resources for upskilling in this area. If you're seeking help around training your workforce, contact us at **skills@hays.com**

Find experienced talent

As a lifelong partner to businesses around the world, Hays are well placed to find the right solutions to your staffing needs. From identifying existing talent to training those with potential, we're working for your tomorrow to help your organisation succeed in the short and long term.

If you'd like to speak with one of our expert cyber security consultants about your team and its strategy, **get in touch today**.

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.

Find out more at expertsintechnology.hays.com