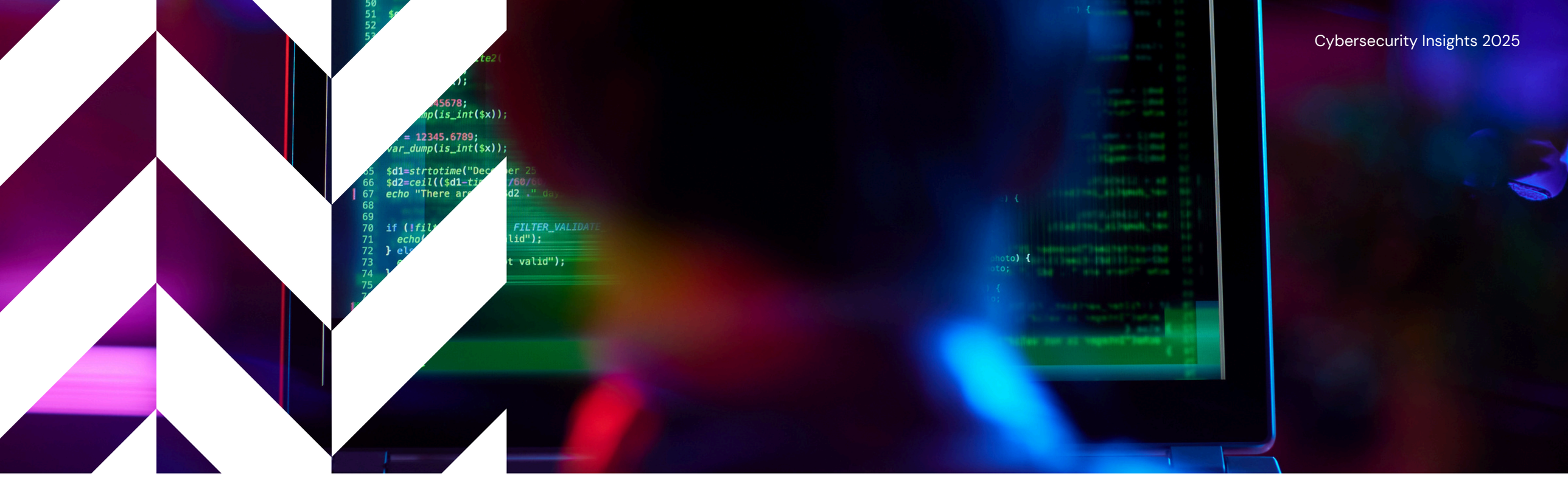
MASON ALEXANDER

Cybersecurity Insights 2025:

Talent, Threats & Readiness



Introduction

At Mason Alexander, we recently surveyed professionals across the cybersecurity industry to better understand how organisations are approaching **cyber readiness**, **threats**, **skills**, and **talent challenges** in 2025.

The findings provide a snapshot of how companies are preparing for the future — highlighting both strengths and areas where pressure is mounting. Even among organisations with dedicated in-house teams, the ongoing **war for talent**, the rise of **AI**, and growing **regulatory pressures** are creating new challenges.

In this insights document, we outline the key findings from our survey, explore their implications for employers, and provide recommendations on how to strengthen cybersecurity strategies through talent and hiring.

- **For hiring managers**, this report offers a view of the biggest challenges your peers are facing — from skills shortages to employee retention — and how you can stay competitive.
- **For job seekers**, it highlights the most in-demand skills, the barriers companies are facing in hiring, and the opportunities opening up across the industry.

MASON ALEXANDER

Key Cybersecurity Insights and Trends 2025

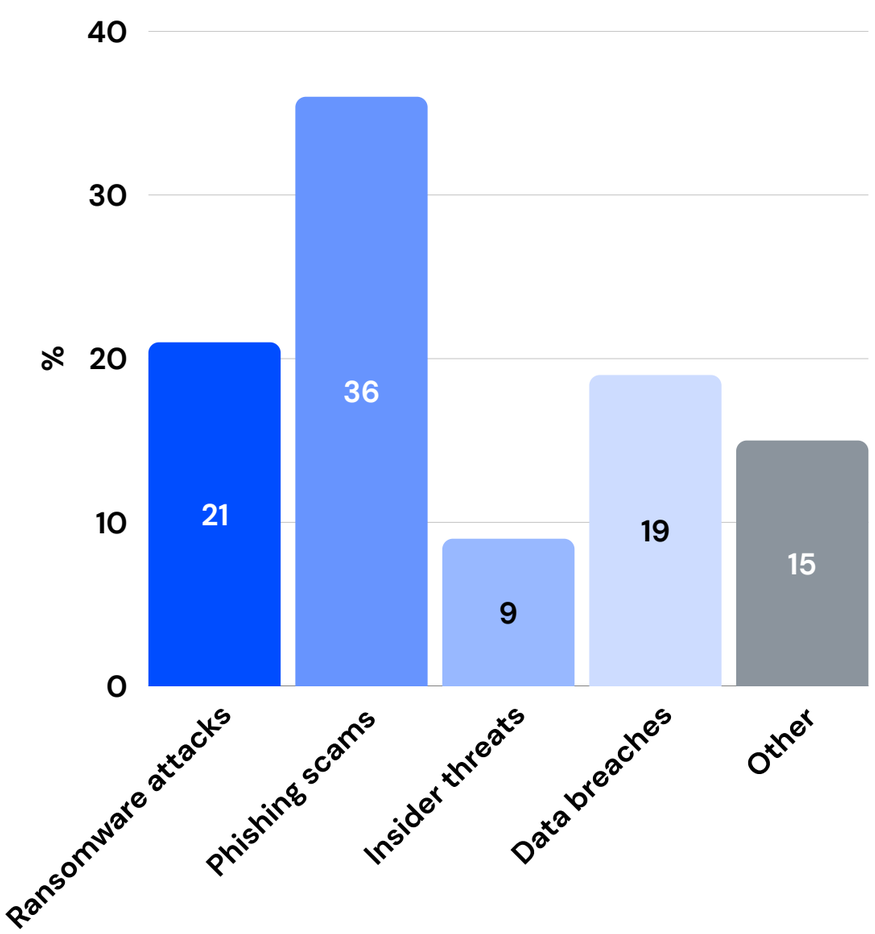
Cybersecurity Maturity: Strong, but Not Without Gaps

72% of respondents reported having a dedicated in-house cybersecurity team — unsurprising given the survey targeted cybersecurity professionals, but still a reassuring sign that businesses recognise the importance of building internal expertise. Encouragingly, **79%** said cybersecurity is frequently discussed at a strategic level, showing that cyber risk is firmly on the boardroom agenda.

However, readiness isn't universal. While **70**% have a fully detailed and tested incident response plan, nearly a **quarter** admitted theirs was incomplete or untested, and **6%** had none at all. In an era of escalating threats, those gaps can be costly.

Recommendation for employers:
Ensure your incident response plan isn't just written but regularly tested. Even strong teams can be caught out without clear, practised procedures.

Biggest Cybersecurity Threats



The Threat Landscape: Human Error Still Leads

When asked about the biggest cybersecurity threats, **phishing scams** (**36%**) and **ransomware attacks** (**21%**) topped the list. Insider threats and data breaches followed, while open responses flagged risks such as **financial fraud**, **third-party vulnerabilities**, and **Microsoft 365 security weaknesses**.

The dominance of phishing underscores that **people remain one of the weakest links in cybersecurity** — even with technical controls in place.

It's encouraging that **77%** of companies run regular training for all employees, but **11%** still provide no training at all, leaving themselves exposed.

Recommendation for employers:
Training must be ongoing and engaging, not a tick-box exercise. Organisations that embed cyber awareness into their culture are far better placed to reduce human-driven risks.

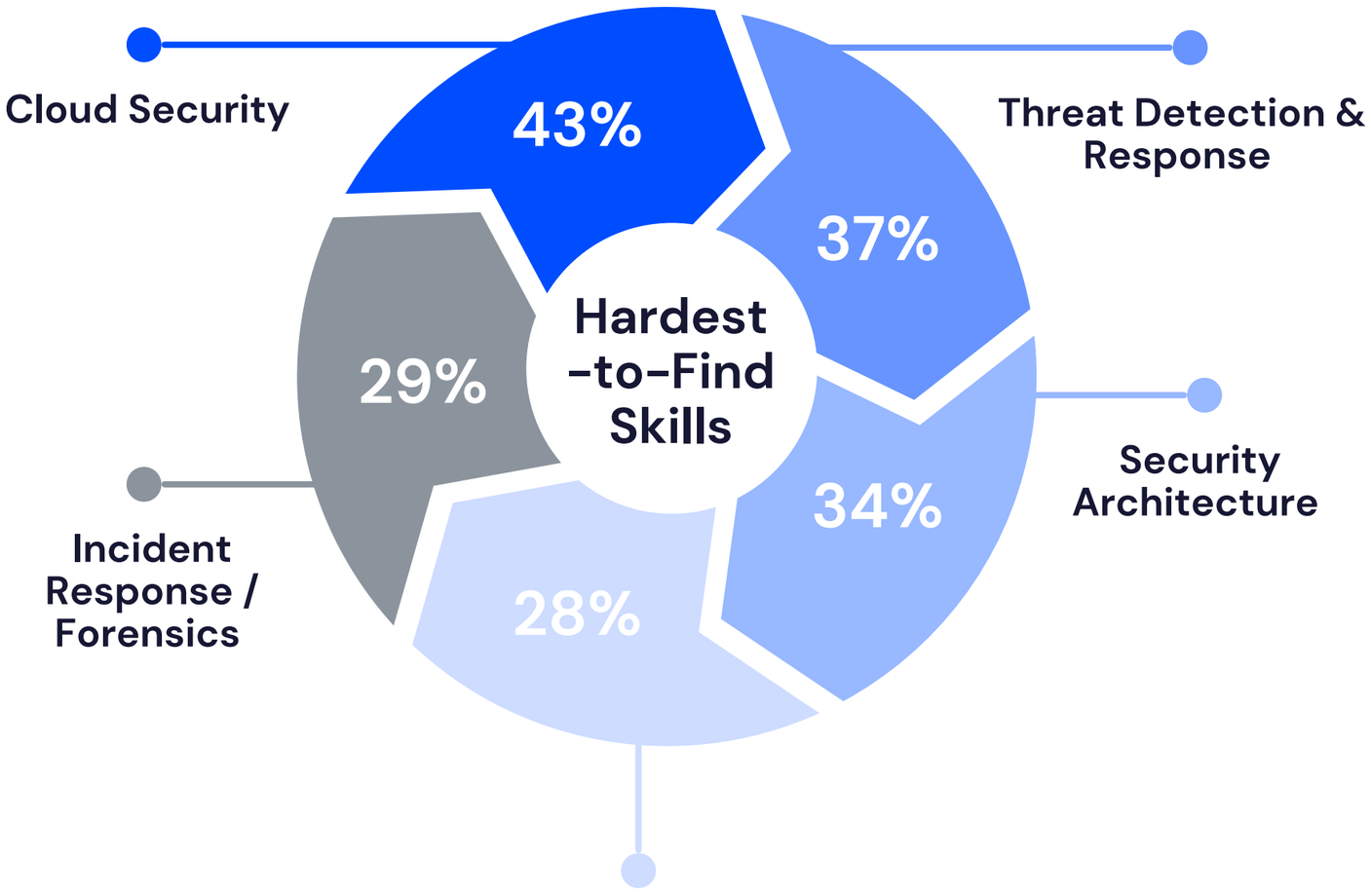
MASON ALEXANDER

Key Cybersecurity Insights and Trends 2025

Hiring Challenges: A Persistent Skills Shortage

Despite the strong presence of in-house teams, hiring remains a major challenge. **83%** of respondents said they face difficulties hiring cybersecurity professionals — with a third describing the challenge as significant.

The hardest-to-find skills reflect today's evolving landscape:



*Above figures represent % of all respondents that selected each hardest-to-fill skill.

32%

stated they face significant challenges hiring cybersecurity professionals.

Other technical skills also ranked as difficult to source, including **penetration testing** (**26%**), secure **software development / DevSecOps** (**19%**), and **Identity and Access Management** (IAM) (**19%**).

In addition, **21%** of respondents highlighted "other" skills gaps, pointing to areas such as **crypto security**, **disaster recovery**, **endpoint protection**, and **Microsoft 365 security skillsets**.

While others emphasised another challenge that often lies in the **mindset** and **cultural fit** of candidates, rather than purely technical expertise.

Key Cybersecurity Insights and Trends 2025

Barriers to Recruiting: Salary Pressures and Market Limitations

When asked about the biggest barriers to hiring cybersecurity talent, the most common challenge cited was a lack of qualified candidates (**43%**), followed by high salary expectations (**21%**) and competition from larger or better-known employers (**13%**).

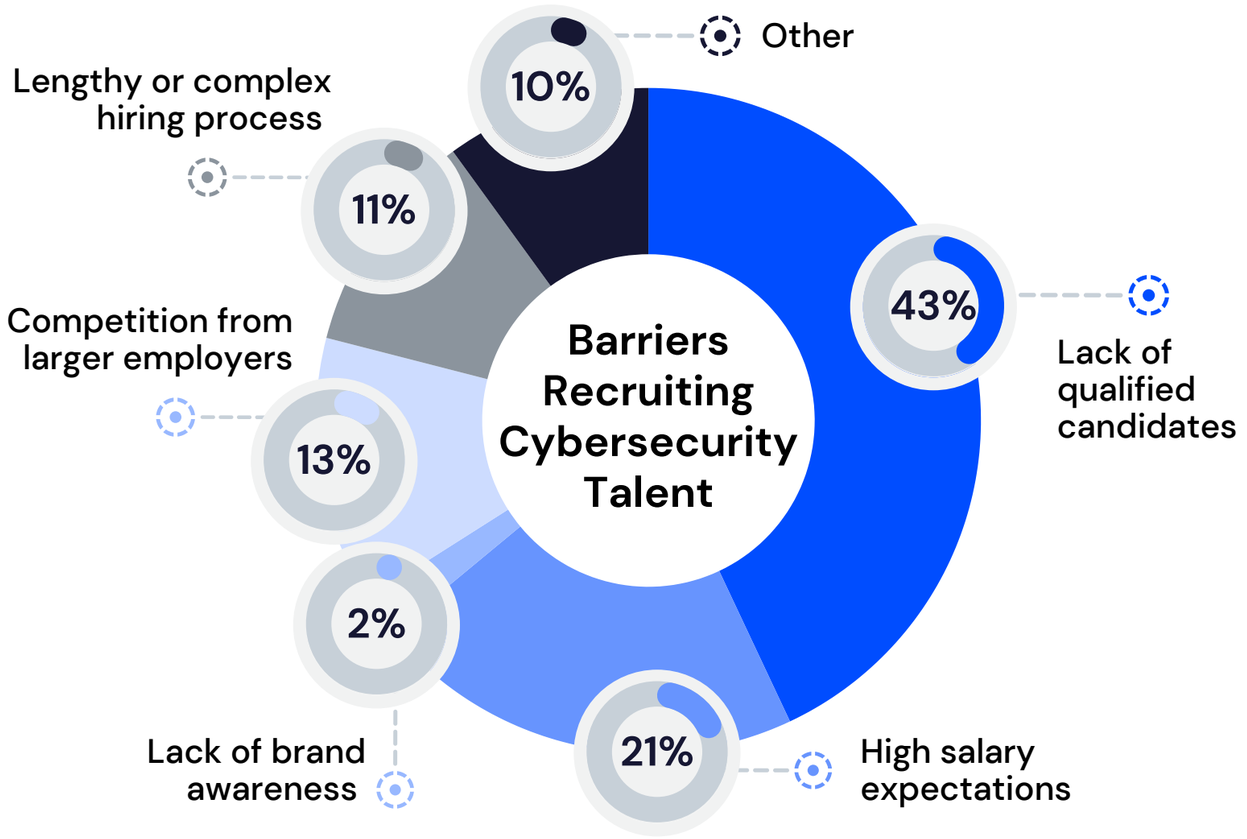
Additional comments under "Other" highlighted similar themes — with some noting that companies often **demand excessive years of experience** for junior roles, which unnecessarily limits the talent pool, while others pointed to a preference to **outsource** rather than hire directly.

These insights suggest that, beyond the tight talent market, **internal hiring expectations** and **processes** can also restrict access to available talent — underlining the importance of more **flexible** and **efficient recruitment strategies**.

We're also seeing a growing shift toward **exclusive recruitment partnerships**. Rather than engaging multiple or generalist agencies, many organisations are choosing to work with specialist firms on an exclusive basis, achieving better outcomes through deeper expertise and more focused searches.

Recommendation for employers:
To attract talent, companies need to be realistic about requirements, streamline hiring processes, and invest in internal upskilling.

Salary remains important, but career growth and flexibility are equally critical to candidates.

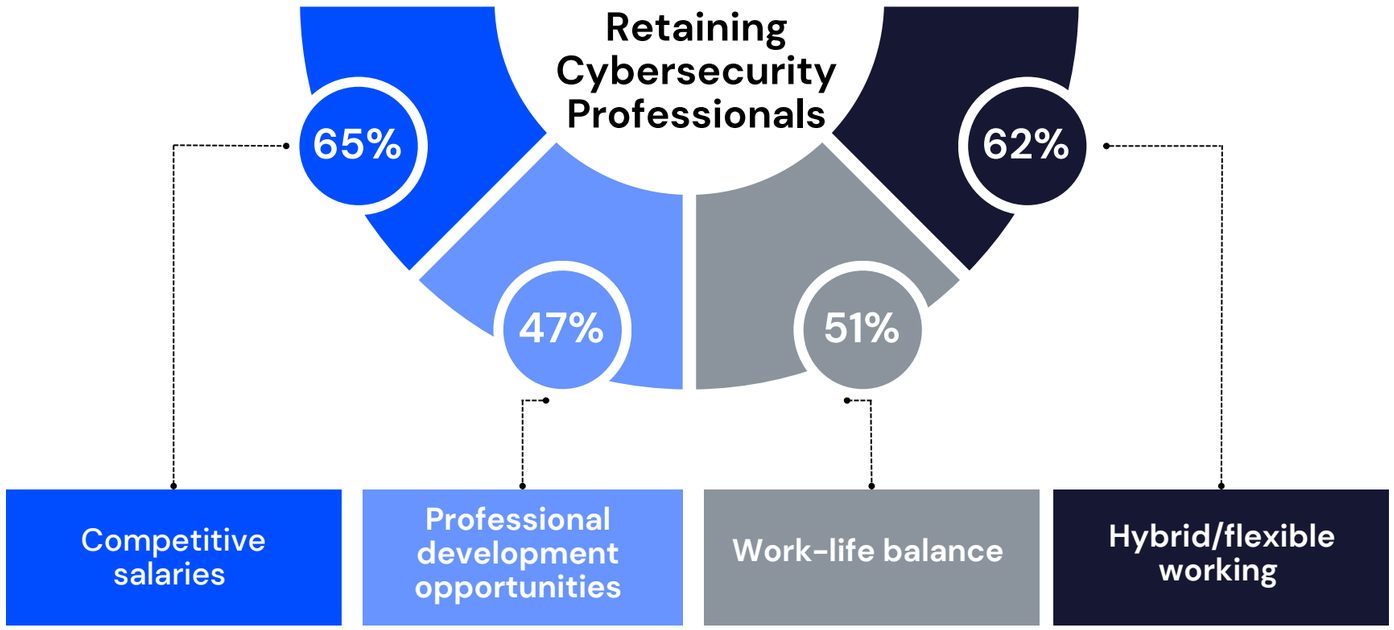


MASON ALEXANDER

Key Cybersecurity Insights and Trends 2025

Retention: Beyond Salaries

Retention is just as important as hiring. The majority of respondents said they focus on:



*Above figures represent % of all respondents that selected each retention strategy for cyber professionals.

Flexibility and development are just as valued as pay. This suggests that retention strategies should balance financial incentives with meaningful growth opportunities and employee wellbeing.

Recommendation for employers:
Retaining cyber talent requires a holistic approach. Flexible working, career pathways, and strong professional development programmes can be as powerful as salary in keeping teams engaged.

Recommendation for employers:
Treat regulatory readiness and AI adoption as competitive advantages.
Companies ahead of the curve will not only be more secure but also more attractive to talent seeking innovative environments.

Regulation & AI: New Pressures, New Opportunities

The upcoming NIS2 Directive is already shaping priorities. While **30%** said they are well prepared and **43%** are preparing, **6%** were unaware of the regulation.

At the same time, AI is entering the cybersecurity toolkit. **38%** of respondents actively use AI-based solutions, while another **38%** are exploring options. Just **23%** aren't engaging with AI at all.

This reflects a growing awareness that AI is both a threat and a defence tool — organisations will need to keep pace to remain resilient.

Key Cybersecurity Insights and Trends 2025

Hiring Outlook: Signs of Demand Ahead

Finally, the hiring outlook shows steady demand. While only **23%** are actively hiring cybersecurity roles right now, a further **40%** plan to within the next 6–12 months. This suggests that despite economic pressures, cybersecurity recruitment will remain resilient as we head into 2026.

For job seekers, this is a clear signal: skills in cloud security, threat detection and security architecture are among the most valuable in the market.

Conclusion: Building Resilience Through Talent

The results of this survey highlight both progress and pressure points in the cybersecurity industry. Organisations are increasingly mature in their approach, but skills shortages, retention challenges, and evolving threats mean there's no room for complacency.

For employers, the key is to:

- Regularly test and update incident response plans.
- Prioritise ongoing, engaging employee training.
- Focus on retention through flexibility, development and wellbeing.
- Stay ahead of regulations and harness AI as a defence tool.
- Consider exclusive partnerships with specialist recruitment firms to secure niche skills more effectively and improve hiring success rates.

For job seekers, the message is clear:

- Cybersecurity remains one of the most in-demand and resilient fields. Building expertise in cloud, security architecture, threat detection and AI-driven defence will place you at the centre of tomorrow's opportunities.

Partnering for Cyber Talent Succes

At Mason Alexander, we specialise in connecting organisations with the cybersecurity expertise they need to stay ahead of evolving threats. Our team partners closely with clients to understand their risk landscape, regulatory requirements, and security priorities — enabling us to deliver the right talent across cloud security, threat detection, governance, security architecture and beyond.

Whether you're building a permanent cyber function, scaling quickly with contract hires, or filling specialist and hard-to-source roles, we have the network and insight to move with speed and precision. Many clients choose to work with us on an exclusive basis, which allows for a more focused search, deeper engagement and higher success rates in securing the right talent. Our strong relationships across Ireland's technology and cybersecurity community mean we can access talent that isn't always visible on the open market.

From start-ups strengthening their first lines of defence to global enterprises navigating regulatory change and AI-driven risks, we provide tailored recruitment strategies that align with your pace, challenges and ambition.

As you plan for the future, Mason Alexander is here to help you secure the cyber talent that will protect, innovate and sustain your organisation's success.

MASON ALEXANDER

www.masonalexander.ie

hello@masonalexander.ie

+353 1 685 4414