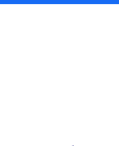


From Shortage to Strength: Fixing the Cyber Skills Gap



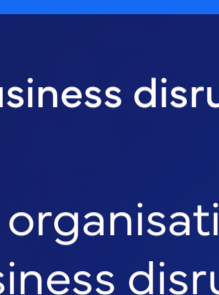
David Clemente
Research Director,
European Security, IDC

Why the shortage of cyber skills is a top concern for organisations today

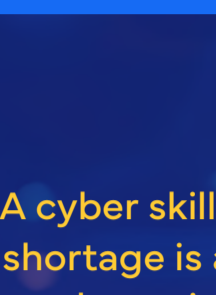
Ransomware is one example that demonstrates how a lack of security skills can be costly.



of ransomware incidents result from **"human error."**



of ransomware incidents result in **"attackers successfully infiltrating data."**



of organisations that paid a ransom paid **"between \$100,000 and \$1 million to regain access to their systems or data."**

And this does not include business disruption.



of breached organisations suffered business disruption lasting from **"a few days" to "more than a few weeks."**

A cyber skills shortage is a clear weakness in many organisations' security postures.

Source: IDC's Worldwide Future Enterprise Resiliency & Spending Survey (FERS Survey), 2025 Wave 5 (n = 885)

Why are organisations struggling to hire and retain cybersecurity talent?



Shortage

Not enough talent to meet demand



Cost

Security budgets regularly constrained



Complexity

New skills needed to secure new technology



The Top 3 challenges to getting the most value from security operations:



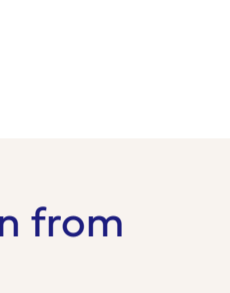
1

The need for 24 x 7 x 365 dedicated staff



2

Expertise needed to fully use the latest security tools



3

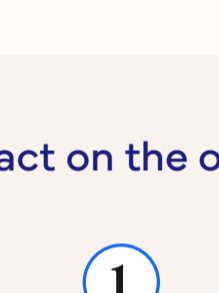
Skills to increase automation across detection and response workflows

Source: IDC's Worldwide Views on SIEM Survey, 2024 (n = 1,004)

Why CIOs and security leaders are concerned about finding the right security specialists



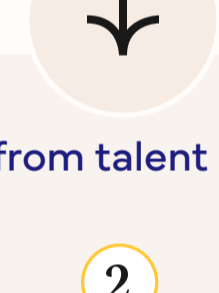
The top 3 CIO obstacles that prevent the IT function from achieving its security goals:



1

AI-driven threats outpacing defences

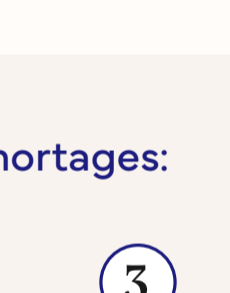
(including the growth of AI-enabled commodity attacks, such as phishing)



2

Cybersecurity talent shortages and skills gaps

(Automation is improving rapidly, but skilled people will always be needed for critical roles.)



3

The growing sophistication of cyberthreats and attackers

(now with added AI)

The cyber skills shortage is a constant top concern for CIOs.

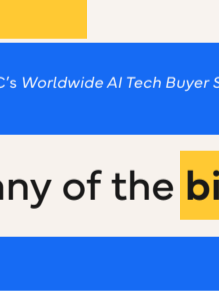
Source: IDC's Worldwide CIO Sentiment Survey, 2025 (n = 437)

The whole organisation suffers when the right people cannot be found

A shortage of people in critical functions, such as security, can damage the broader business in multiple ways.



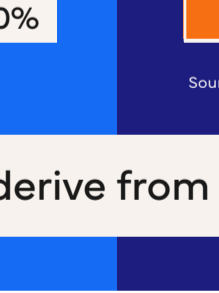
Impact on the organisation from talent and skills shortages:



1

42%

It takes us longer to fill vacant positions (introducing risk).



2

40%

We have difficulty in retaining top talent (disrupting plans).



3

35%

Digital transformation initiatives are delayed (slowing security investment).

Source: IDC's Worldwide FERS Survey, 2025 Wave 5 (n = 885)

Speed of change: The security and technology landscape is changing too fast for organisations to rely only on in-house talent

For example, AI adoption, cloud configuration, and the resulting security risks are creating a high demand for associated security skills.

Biggest business risks of adopting agentic AI:



Source: IDC's Worldwide AI Tech Buyer Survey, 2025 (n = 2,296)

Skills that organisations lack and/or find difficult to hire:



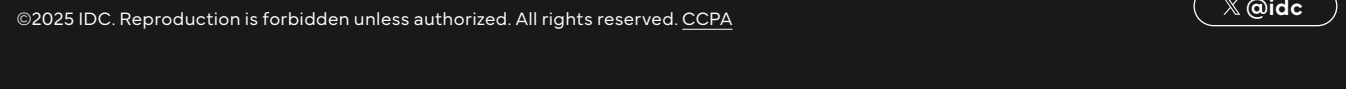
Source: IDC's Worldwide CEO Perspective on Technology Survey, 2025 (n = 419)

Many of the **biggest risks** derive from a **skills shortage**.

From shortage to strength: How to fix your organisations cyber skills gap

Managed security services offer efficiency and effectiveness. They also provide levels of responsiveness and scalability that are impossible for most organisations to achieve in house.

Will those organisations that need to strengthen the monitoring or management of their cybersecurity tools consider a third party to do this?



48% are convinced of the benefits of managed security services.

27% need to consolidate tooling first.

25% will try to grow the internal security team.

■ Yes, we are looking for a suitable third-party provider.
■ Yes, we have already engaged one and are now considering replacing it with a better third-party provider.
■ No, we need to consolidate some security tools first.
■ No, we will increase in-house headcount to manage our security tools.

Source: IDC's Worldwide Security Services Survey, November 2024 (n = 275)

The benefits of managed security services are valuable for organisations of all sizes

Access to talent

They benefit from accessing rapidly scalable teams with a breadth of security expertise.

Flexible cost

They gain greater cost efficiency and budget flexibility, which are particularly valuable for rapidly adding or scaling services.

Peace of mind

They gain confidence that a rapid and increasingly automated response can address compliance requirements and mitigate the potential impact of incidents.