AI and quantum readiness reshape cyber resilience in the Middle East

2026 Global Digital Trust Insights: Middle East findings

As the Middle East accelerates digital transformation – from AI to quantum-ready security – organisations are increasing investment and strengthening board-level focus on cyber, making trust and innovation essential to sustaining growth.

Contents

Introduction

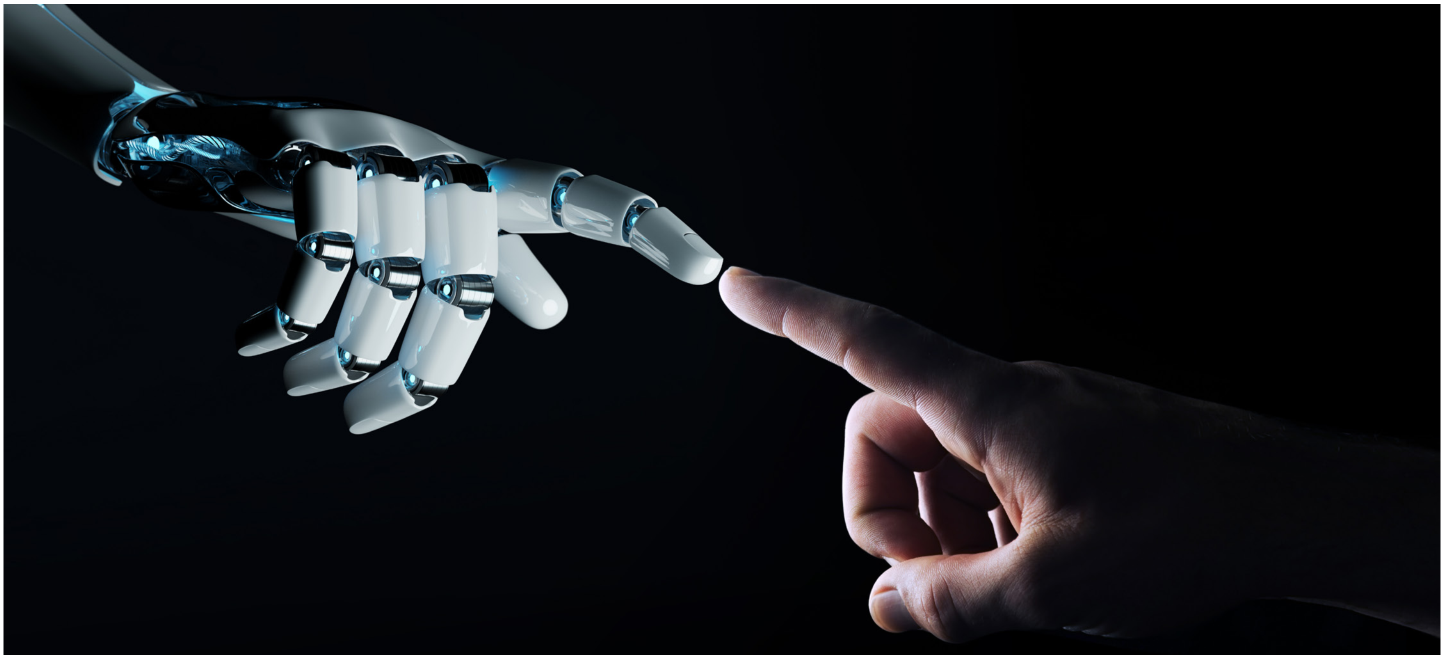
The Middle East has entered a new phase in its cybersecurity journey. Having established the foundations of resilience, organisations are now scaling investment and embedding security at the heart of strategic decision-making. What was once a defensive safeguard is increasingly recognised as a catalyst for competitiveness and growth.

Artificial intelligence (AI) is moving rapidly from experimentation to deployment, opening new possibilities for stronger defence while reshaping how organisations operate. Cloud adoption and data modernisation are expanding digital capacity and interconnectivity, bringing greater agility and speed to transformation. At the same time, boards and leadership teams are working more closely with chief information security officers (CISOs), ensuring that cybersecurity is fully integrated into enterprise strategy.

Yet progress brings new challenges. The region's enthusiasm for new technologies broadens the attack surface, while integration challenges around AI highlight the difficulty of moving from ambition to execution. Governance gaps and human error remain persistent vulnerabilities that can undermine even sophisticated investments.

Our survey findings reflect a region advancing in parallel with national transformation programmes and economic diversification – a broader context that is helping to amplify momentum around digital trust and security. Cybersecurity is no longer just about protection – it is about enabling trust, resilience and innovation in economies that are advancing faster than their global peers. With early steps into areas such as AI governance and quantum readiness, the Middle East is building the capabilities needed to keep pace. This will be essential in a rapidly changing digital landscape.

Taken together, these findings show rising budgets, CEO-CISO alignment, early moves into quantum and a shift from reactive defence to proactive resilience. The overall picture is of a region moving with confidence and ambition, committed to digital trust. To sustain this momentum, leaders will need to make choices about where to focus their efforts next.



Key findings

62%

of Middle East respondents expect their cyber budgets to increase in 2026, compared to 50% globally

88%

of organisations in the region are already measuring the potential financial impact of cyber risks

53%

of Middle East organisations cite lack of knowledge as the biggest barrier to adopting AI for cyber defence, compared to 50% globally

50%

of respondents in the region are prioritising AI and machine-learning tools to address cyber talent gaps over the next 12 months

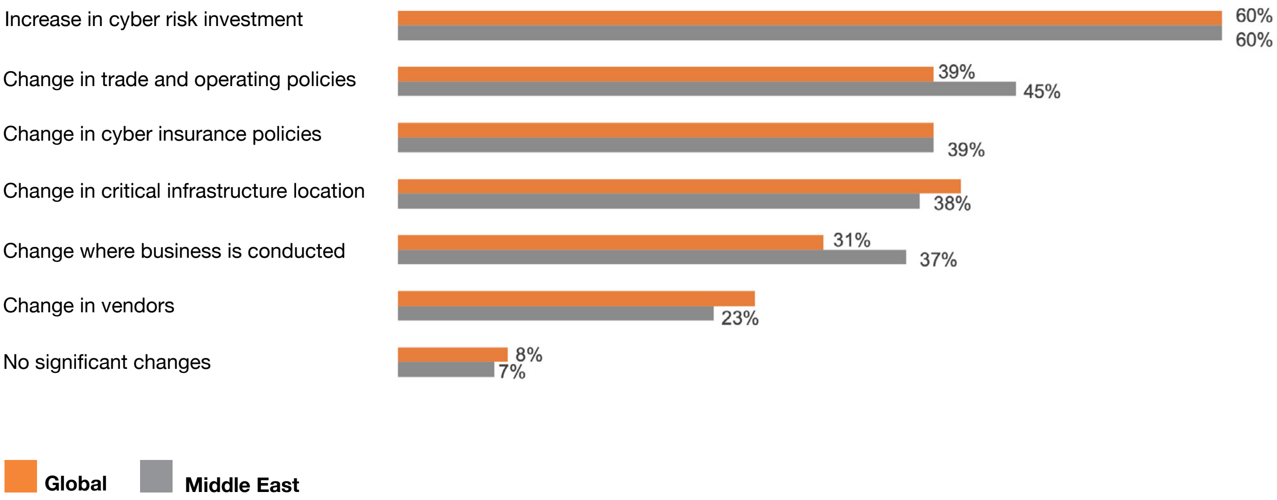
30%

of organisations in the region are planning to implement responsible AI practices in the next 12 months, compared with 23% globally

Digital and cyber risks stay at the top of the agenda

Organisations across the Middle East continue to rank digital and cyber risks above other concerns. When asked over the next 12 months, which of the following areas within their organisation's cyberstrategy is changing in response to the current geopolitical landscape, 60% of Middle East business and tech leaders, in line with their global peers, reported 'increase in cyber risk investment' among their top three cyber strategy priorities. This indicates that regional organisations recognise cyber as a frontline risk and a core business resilience priority.

Over the next 12 months, which of the following areas of your organistion's cyberstrategy is changing in response to the current geopolitical landscape?



Several industries in the Middle East already face heightened exposure to cyberattacks, with government institutions, energy companies, financial services and telecommunications providers among the most vulnerable. For example, the energy sector's heavy reliance on operational technology makes it a prime target for such attacks, while financial institutions face persistent threats from phishing and data breaches as digital transactions surge. At the same time, telecom companies must contend with broader attack surfaces created by 5G and satellite internet expansion.

The region is adopting a multilayered defense strategy, combining sustained investment in infrastructure and monitoring, stricter security standards, and regulatory mandates to ensure that digital transformation is matched by strong cyber resilience.[1]

Policy and operating model changes also featured prominently as part of the findings, with 45% of respondents (vs. 39% globally) indicating that "change in trade and operating policies" were among their top three priorities, while almost 40% said they were updating their cyber insurance policies. Insurers and underwriters are also reacting to this evolving risk landscape, and are responding by adjusting coverage terms, exclusions and risk assessment practices in the MENA context.[2] As a result, companies may find that previously covered risks are now excluded, thresholds to trigger claims have risen, and greater ambiguity exists around what is and isn't covered.

Only 7% of Middle East respondents reported "no significant changes," compared with 8% globally, which reinforces that most regional organisations are actively adapting their cyber strategies in some way, rather than taking a "wait and see" approach.

[1] https://www.arabnews.com/node/2600834 [2] https://www.kennedyslaw.com/en/thought-leadership/article/2024/cyber-insurance-in-the-mena-region/

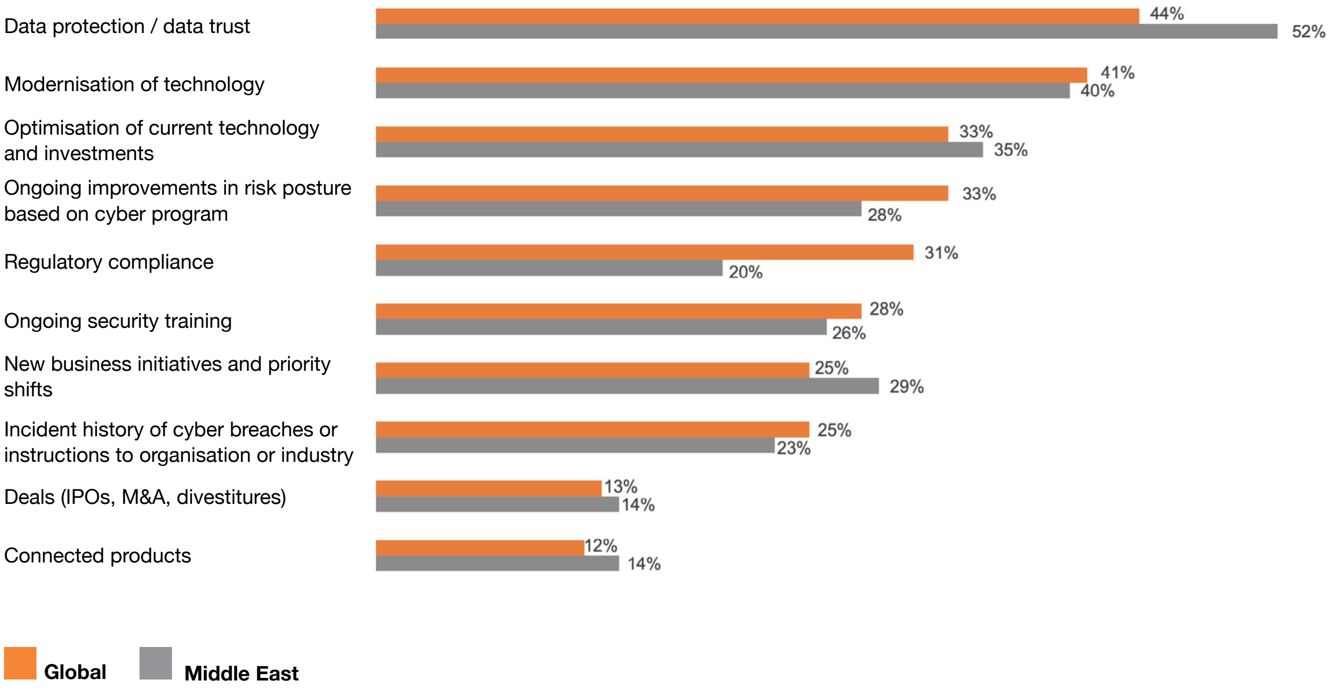
Rising budgets and stronger boardroom focus

Cybersecurity spending is set to continue rising in 2026, with 80% of regional respondents saying their organisations will increase their cyber budgets and a quarter of them expect budget increases of 11% or more, compared with 17% globally. This reflects strong board commitment and recognition that digital trust is now essential for competitiveness. Half of CISOs in the region are now providing cybersecurity programme insights directly to the CEO to inform strategic decisions – compared with 46% globally and nearly half (48%) are meeting regularly with the board, in line with their global peers.

Last year, the emphasis was largely on oversight; this year, this provides clearer evidence of CISOs acting as genuine partners in enterprise strategy. The narrative is shifting from compliance and reporting to active collaboration at the executive level, embedding cyber within core business decisions.

In the Middle East, the key factors influencing cyber spend priorities over the next 12 months are data protection or data trust (52%), modernisation of technology (50%) and optimisation of current technology and investments (40%).

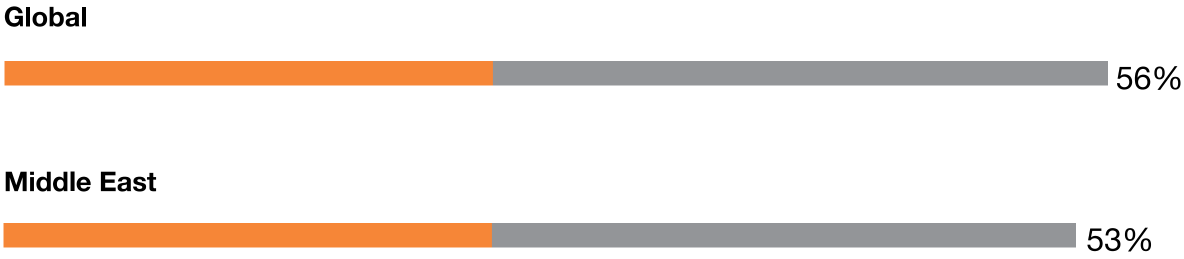
Which of the following factors are influencing your cyber spend priorities over the next 12 months?



Resilience shaped by a proactive mindset

Resilience remains a defining theme. In last year's survey, more than 40% of organisations in the region had already established dedicated resilience teams – significantly higher than 28% globally. This year over half (53%) of Middle East respondents say they are prioritising proactive cybersecurity strategies over reactive approaches, close to the global average of 56%. This indicates that resilience is now seen as a strategic business priority, extending beyond the technical domain to shape wider organisational decision-making. The emphasis on proactivity also reinforces that speed of response is now considered as important as the strength of defences.

Is your organisation spending more resources on reactive or proactive cybersecurity measures?



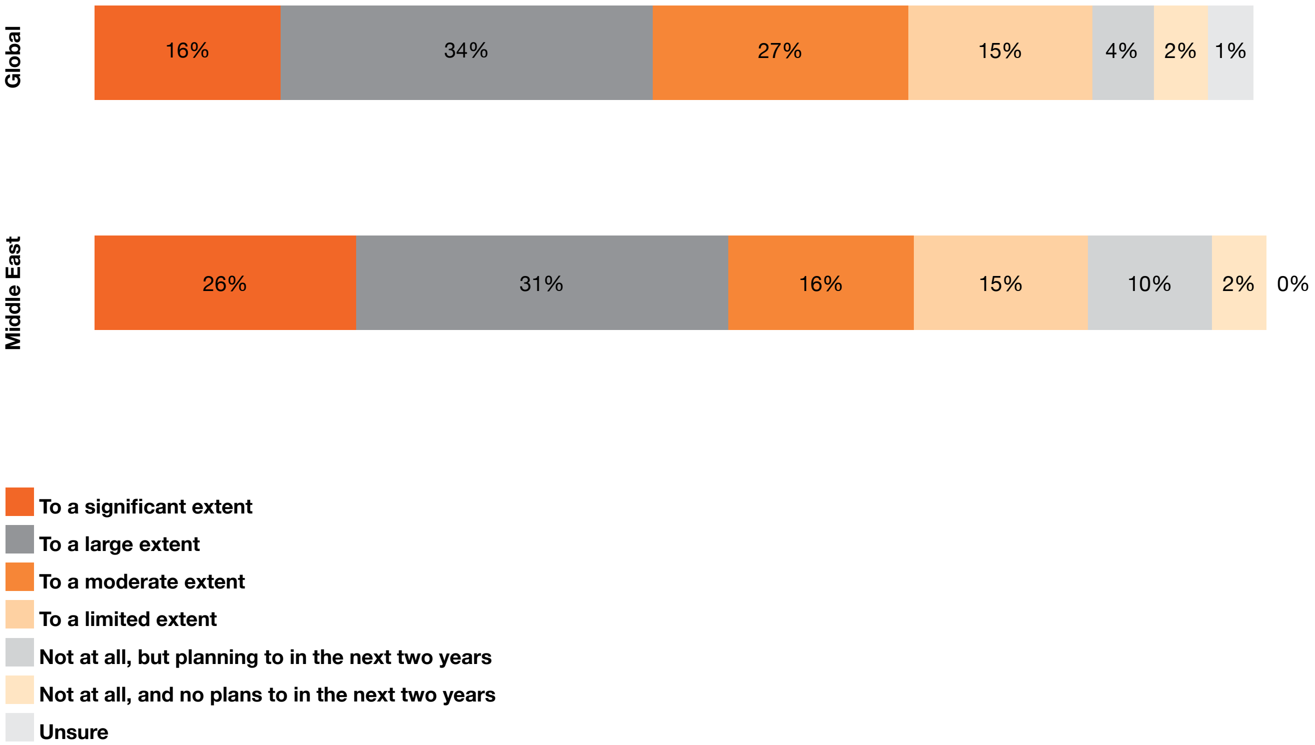
Data breaches highlight financial exposure

In the Middle East, 57% of respondents indicated that their organisation is already measuring the potential financial impact of cyber risks to a large or significant extent, well above the global average of 50%. This reflects growing recognition that cyber threats are now recognised as business risks.

The costs are already visible. Almost a quarter (23%) of respondents in the Middle East reported that the most damaging breach in the past three years cost their organisation US$1m or more. Only 17% of survey respondents said they had not experienced a data breach during that period – broadly in line with the global figure of 18%.

The finding underlines both the financial scale of incidents in the region and the reality that breaches are now increasingly common. In fact, the Middle East now ranks second globally for the average cost of a data breach, estimated at over US$7m per incident.[3]

To what extent is your organisation currently measuring the potential financial impact of cyber risks (i.e., risk quantification)?



[3] https://solutions.fixed.global/en/news/cybersecurity-trends-in-the-gulf-region-for-2025

Data breaches highlight financial exposure

Survey findings indicate that organisations understand that building resilience starts with knowing and trusting data. While data quality ensures accuracy, cataloguing provides visibility of where sensitive information resides and together, they can reduce the risk of breaches. In the region, 30% of business and tech leaders have implemented data quality capabilities across their organisations, lower than the global average of 41% - while 18% plan to do so in the next 12 months, almost same as their global peers.

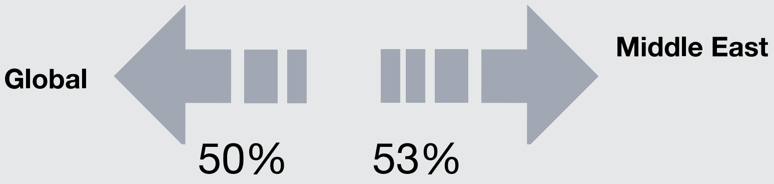
By contrast, the region is on par with global peers in data discovery and cataloguing, with 41% already implementing these capabilities. Notably, 27% of regional organisations are planning to adopt cataloguing in the next year, significantly higher than the global average of 16%. This suggests that recognise the importance of visibility and control over data assets and are accelerating investment in this area.

AI adoption brings new challenges

In the Middle East, more than half of respondents (53%) cited a lack of knowledge in applying AI to cyber defence as one of their top three internal challenges, broadly in line with 50% globally. A further 37% in the region pointed to a shortage of relevant skills, underlining the human capital dimension of AI adoption. Without closing knowledge gaps, organisations risk deploying AI that is poorly integrated, error-prone and vulnerable to misuse. Those that get it right will gain faster detection, stronger resilience and a decisive competitive edge.

What have been your organisation's biggest internal challenges to implementing AI for cyber defence over the last 12 months?

Lack of knowledge in AI for cyber defence



So how are organisations planning to close cyber talent gaps. Half of regional respondents (50%) ranked machine-learning tools and AI among their top three priorities for addressing workforce shortfalls, almost identical to 53% globally. By contrast, only 34% cited upskilling and reskilling and 28% indicated traditional talent recruitment, reflecting a clear tilt towards digital and automated solutions as the preferred path to close talent gaps and sustain trust.

The next step for many organisations is to move from addressing talent shortages to embedding governance around how AI is deployed – a shift that will define the region's approach in the coming year.

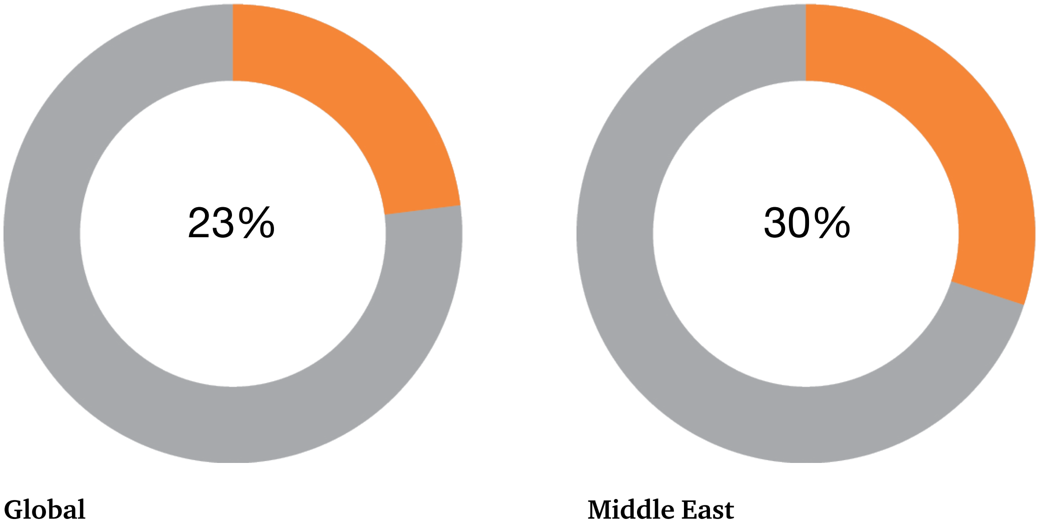
Embedding responsibility into AI adoption

Responding to these challenges requires more than investment in tools – it demands governance frameworks that guide how AI is deployed across the enterprise. Organisations are discovering that effective adoption depends on harmonising data, systems and processes rather than relying on isolated solutions. The Middle East continues to show ambition, but leaders now recognise that success will come from embedding AI into operational reality.

In the region, 30% of organisations say they are planning to implement responsible AI practices in the next 12 months, compared with 23% globally. That both groups identify responsible AI as their top planned measure highlights how quickly it has become central to enterprise-wide data risk management.

To what extent has your organisation implemented or is planning to implement any of the following measures to address data risk across the enterprise?

Middle East leads in planning for responsible AI



Global

Middle East

For Middle Eastern leaders, the emphasis on responsible AI reflects not only rapid adoption of new technologies but also an understanding that governance, trust and accountability must evolve in parallel.

Preparing for the quantum era

Quantum computing has shifted from a distant concern to a growing priority. In the Middle East, 27% of organisations report progress in implementing quantum-resistant security measures, compared with 22% globally, while another 27% are at the “piloting and testing” stage. If widely used encryption standards are broken by quantum advances, everything from national payments systems to cross-border trade flows could be exposed. That’s why leaders in the region are already piloting quantum-resistant measures, years ahead of necessity. This represents a clear step forward from last year, when quantum readiness was discussed largely in terms of future intent.

How far along is your organisation when it comes to quantum-resistant security measures?

27%

of respondents in the Middle East report progress in implementing quantum-resistant security measures.

The regional lead reflects both strong regulatory signals and a proactive mindset among business leaders. By taking early steps towards quantum-resistant security, organisations in the Middle East are positioning themselves ahead of the curve – an essential move given the long lead times required for cryptographic transitions in complex digital environments. For business leaders, those who start now will be better placed to manage the risks and opportunities of the quantum era.

Actionable insights for business and tech leaders

To sustain momentum and turn progress into lasting advantage, organisations must make deliberate choices about where to focus. The 2026 survey highlights five priorities that can help leaders embed digital trust more deeply into their businesses and prepare for the next wave of transformation.

Embed cybersecurity into every strategic decision: Budgets are rising and CISOs are closer to the C-suite, but cyber risk still needs to be factored into all major business decisions. Leaders should ensure security considerations are fully integrated into growth strategies, operating model shifts and investment planning.

Focus on proactive resilience: There is a clear opportunity to strengthen resilience further. Faster detection, response and recovery should be embedded across operations, supported by investment in automation and playbooks that shorten reaction times.

Determine if your business should leverage managed services: Assess the long-term costs of reacting to security incidents versus investing proactively in managed services by developing an ROI-based managed services plan that maps technology, skills and resource needs.

- **Address the integration challenge of AI:** AI is moving from promise to practice and integration is now the most significant barrier. Organisations should develop clear frameworks for embedding AI into existing technology stacks, while investing in training and governance to reduce risks of error and misuse
- **Accelerate readiness for quantum:** Early steps towards quantum-resistant security are evident in the region, but the transition will be long and complex. Business leaders should ensure that migration plans are in place now, supported by continuous assessment of cryptographic dependencies across their digital infrastructure
- **Close the gaps in governance and collaboration:** Leadership involvement has strengthened, yet governance weaknesses and silos between business units and cyber teams still pose risks. Boards, CISOs and functional leaders should reinforce cross-enterprise collaboration, aligning cyber strategy with risk management, finance and operations to create a unified approach

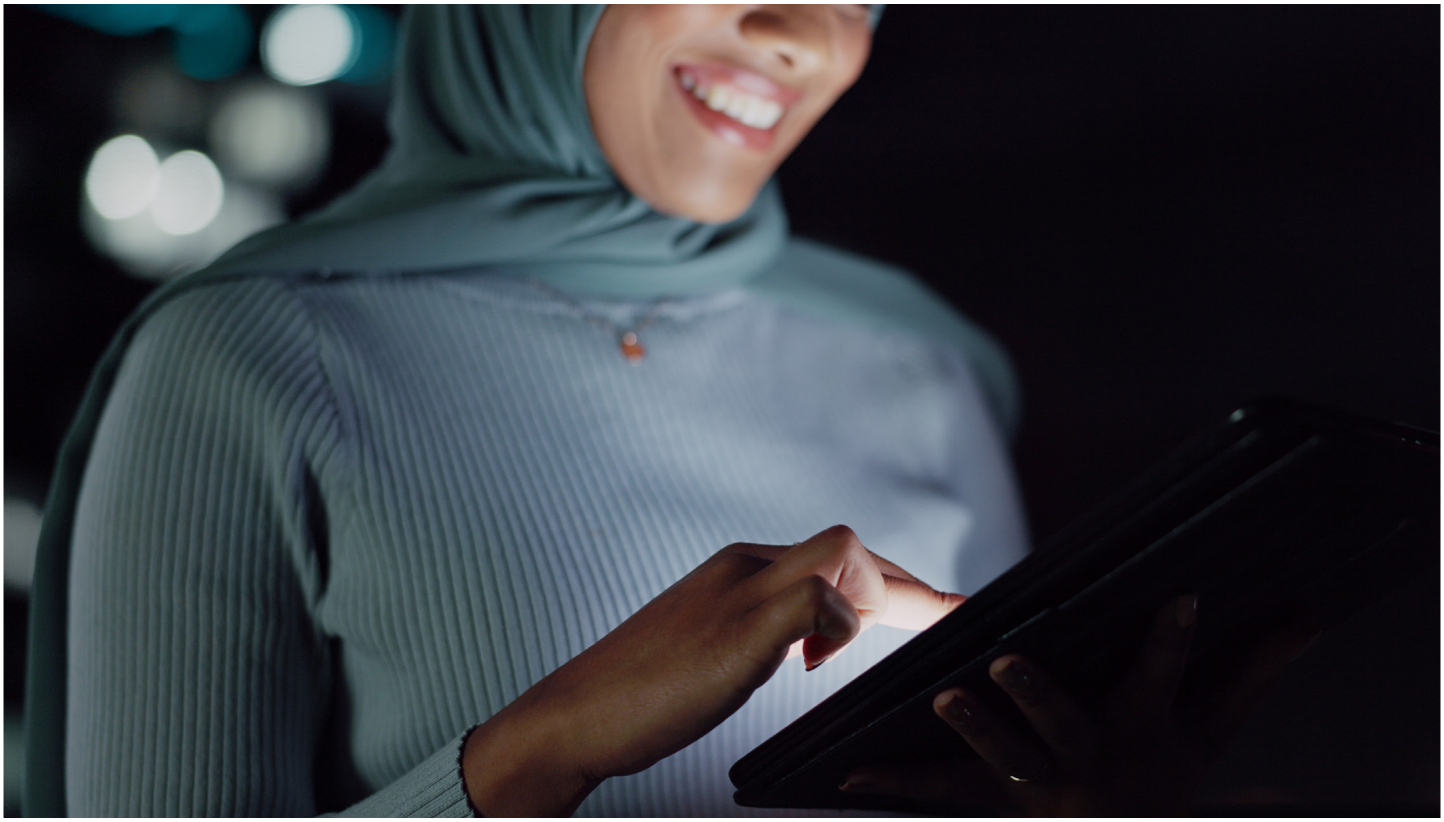
> “
>
> Cybersecurity has become the foundation of digital transformation. By harnessing AI and preparing for quantum, organisations in the Middle East are building trusted systems that can power economies for decades to come.”

Samer Omar
Cybersecurity and Digital Trust Leader,
PwC Middle East

Cyber matures in the Middle East – year-on-year progress

Findings from the 2025 and 2026 surveys show how the region has moved from building the foundations of cyber resilience to embedding it more deeply into leadership and operations:

- **Budgets move mainstream:** Last year almost a quarter of organisations planned double-digit increases in cyber budgets. Now, 62% now expect overall budget growth of 5% or more, signalling that investment has shifted from selective to mainstream
- **CISOs broaden their role:** Last year, CISOs were mostly engaged with CFOs on cyber investment. This year, 50% are providing programme insights directly to CEOs, showing a pivot from financial oversight to shaping enterprise strategy
- **Resilience matures:** Last year, nearly half of organisations had set up dedicated resilience teams. Now the emphasis has moved to operations, with 58% prioritising proactive over reactive (36%) measures, embedding resilience into day-to-day activity
- **AI moving from hype to integration:** Last year, 83% expected to deploy GenAI for cyber defence within 12 months, far ahead of the global average. This year, 53% cite lack of knowledge and 37% a shortage of skills as key barriers, marking a shift from optimism to the practical realities of implementation



Managed services as a strategic accelerator

AI and cloud are not only the top cybersecurity investment areas, they're also the top use cases for specialised managed security services. Organisations are using managed services for more than outsourcing capabilities. They're partnering with providers to modernise the way critical systems are delivered.

Managed services are becoming strategic accelerators, stepping in to compensate for skills shortages while delivering speed, scale and specialised knowledge. In a threat environment that's growing more complex by the day, they provide a way to modernise defences without diverting focus from innovation and growth.

- 21% of organisations globally put cyber managed services in their top-three priorities for investment over the next 12 months[4]
- To address cyber talent gaps, 42% of organisations in the Middle East ranked managed services among their top-three priorities – higher than the 39% global average
- Significantly, 48% of global organisations that have experienced a major attack are prioritising managed services to address cyber talent gaps[5]

> “
> Managed services are now central to how organisations tackle cyber risk. They deliver the expertise and agility needed to confront increasingly sophisticated threats. By closing talent gaps and modernising defences, managed services allow businesses to stay secure while keeping their focus on innovation and growth.”

Bala Chandran
PwC Middle East Partner and Managed Services Leader

[4] https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html

[5] https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html

Contact us

Samer Omar

Cybersecurity and Digital Trust Leader, PwC Middle East

samer.omar@pwc.com

About PwC

At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 370,000 people in 149 countries. Across audit and assurance, tax and legal, deals and consulting we help build, accelerate and sustain momentum. Find out more at www.pwc.com.

With over 12,000 people across 12 countries in 30 offices, PwC Middle East combines deep regional insight with global expertise to help clients solve complex problems, drive transformation, and achieve sustained outcomes. Learn more at www.pwc.com/me.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.