2025 Global Digital Trust Insights:

Middle East findings

With the Middle East advancing in AI and cloud technologies, achieving cyber resilience has become more critical than ever. Business leaders must integrate robust cybersecurity measures into strategic planning, advocate for stronger regulatory frameworks and address emerging risks by adopting new technologies to secure the future of their organisations.

Introduction

In the Middle East, rapid advancements in artificial intelligence (AI), widespread adoption of cloud technologies and a shifting regulatory landscape - coupled with an expanding IT attack surface - mean achieving cyber resilience is now more critical than ever.

This urgency is underscored by the findings of the 2025 Global Digital Trust Insights: Middle East findings, which has surveyed 121 business and technology leaders from the region. It reveals a robust confidence in the region's proactive cybersecurity measures. Nearly half of the organisations already have dedicated resilience teams in place – well above the global average.

As the region accelerates its digitisation efforts, fuelled by ambitious national transformation programmes, cybersecurity becomes essential to safeguarding economic growth and innovation. But progress also brings new vulnerabilities and threats. Significant gaps remain, with many organisations still unprepared for cloud related threats, hack-and-leak operations, and third-party breaches.

Additionally, slow response times and limited collaboration between cybersecurity teams and other business functions expose further risks. While there is a need to integrate cybersecurity into strategic planning at the organisation level, executives must collaborate with regional leaders and push for a stronger unified regulatory framework to mitigate evolving threats and ensure the region's continued digital success.

Our 2024 report had also identified critical cyber risks, including the need to strengthen controls across all areas, such as identity and access management[1]. Mitigating cyber risks were a top priority for almost half of the regional respondents, even surpassing concerns about macroeconomic volatility, inflation, and geopolitical risks.

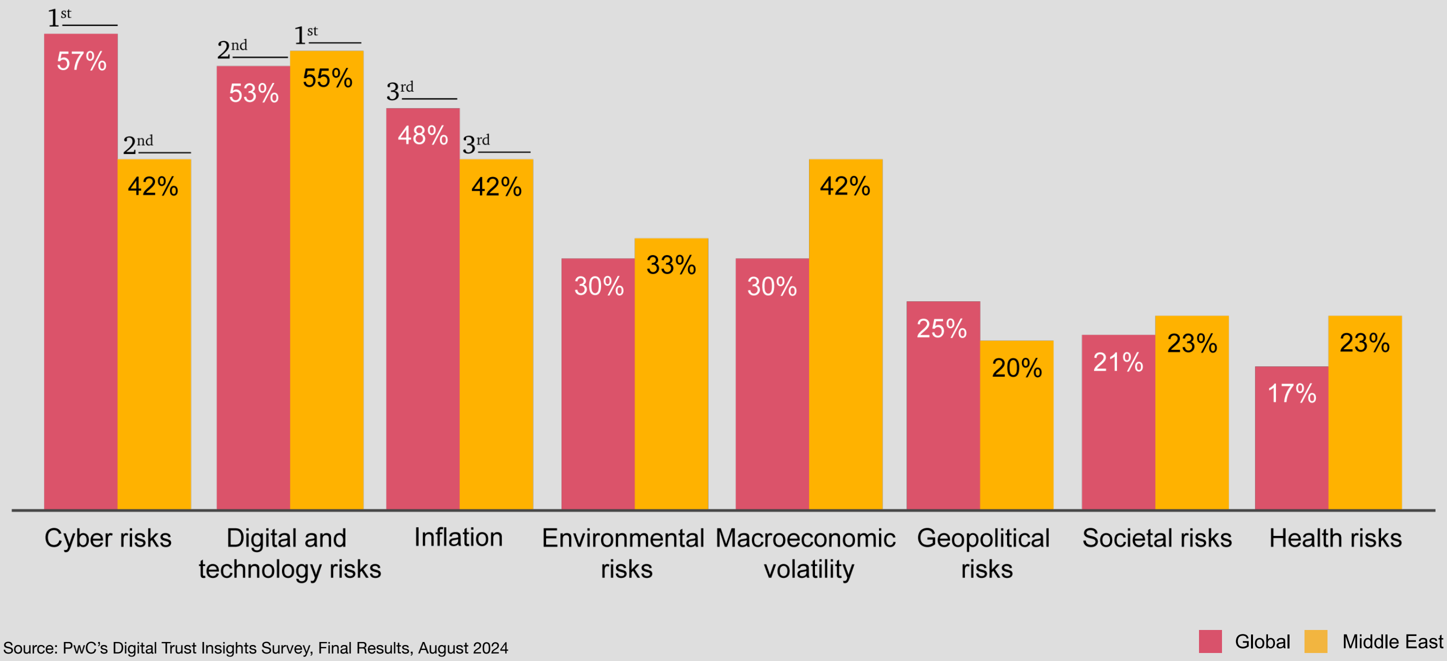
Key findings:

55%	of regional respondents prioritise digital and technology risk mitigation over the next 12 months, compared to 53% globally.
47%	express concerns over hack-and-leak operations, compared to 38% globally.
63%	indicate that organisation boards in the region are highly effective in executing regulatory responsibilities, significantly higher than the 50% globally.
40%	of technology leaders rank data protection as the top investment priority, significantly higher than 28% globally.
33%	of regional organisations report GenAI has expanded their cyber-attack surface, and 48% highlight concerns over the deliberate misuse of GenAI by employees.

Digital and cyber risks continue to take centre stage for Middle Eastern organisations

Digital and technology risks take centre stage for organisations in the Middle East, with 55% of respondents of our 2025 Digital Trust Insights survey prioritise mitigation of these risks over the next 12 months, compared to 53% globally. Cyber risks follow closely, with 42% of organisations in the region prioritising them for the next year. An equal number focused on inflation (42% vs 48% globally) and macroeconomic volatility (42% vs only 30% globally), significantly higher than 20% of organisations who view geopolitical risks as a key concern.

Which of the following risks is your organisation prioritising for mitigation over the next 12 months?



Source: PwC's Digital Trust Insights Survey, Final Results, August 2024

These findings mirror the sentiments of organisations last year, as we had seen in our 2024 Digital Trust Insights: Middle East findings[2]. Last year, mitigating cyber risk was a top priority for Middle Eastern businesses, with 45% of respondents in the region (vs 43% globally) identifying it as a key focus, higher than microeconomic volatility, inflation and geopolitical risks. As regional governments accelerate their digital transformation agendas and prepare for future economies, digital technology is becoming a critical enabler in the Middle East. GCC countries, such as the UAE, Saudi Arabia and Qatar are attracting attention and investments from global tech companies, such as Google, Microsoft and Amazon, highlighting increasing investor confidence in the region.

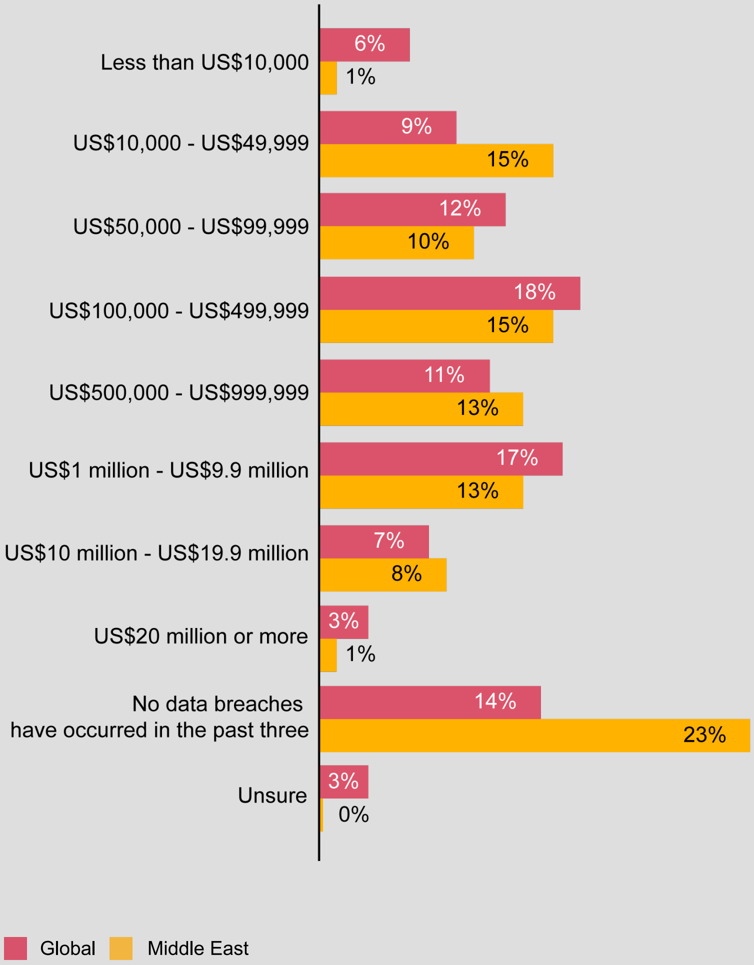
However, the keenness of the region to embrace new technologies also brings heightened risks, prompting organisations to prioritise mitigating tech disruptions, which are seen as both a critical challenge and an opportunity in the region's rapidly evolving digital landscape. Amid a challenging geopolitical climate that heightens cyber threats, critical infrastructure in the UAE and the broader Middle East remains as prime targets, making it imperative for the entire ecosystem to engage proactively in reducing the region's vulnerability to these threats[3]. We see this sentiment echoing in our survey where digital and cyber risks rank higher than inflation and macroeconomic volatility, implying that organisations are trying to strike the delicate balance between driving digital advancement and managing associated risks in a rapidly evolving scenario. This concern was also seen early in the year among regional business leaders in our latest 27th Annual CEO Survey, Middle East findings, where 30% of regional CEOs considered cyber risks a key threat[4].

Unprepared for critical cyber threats

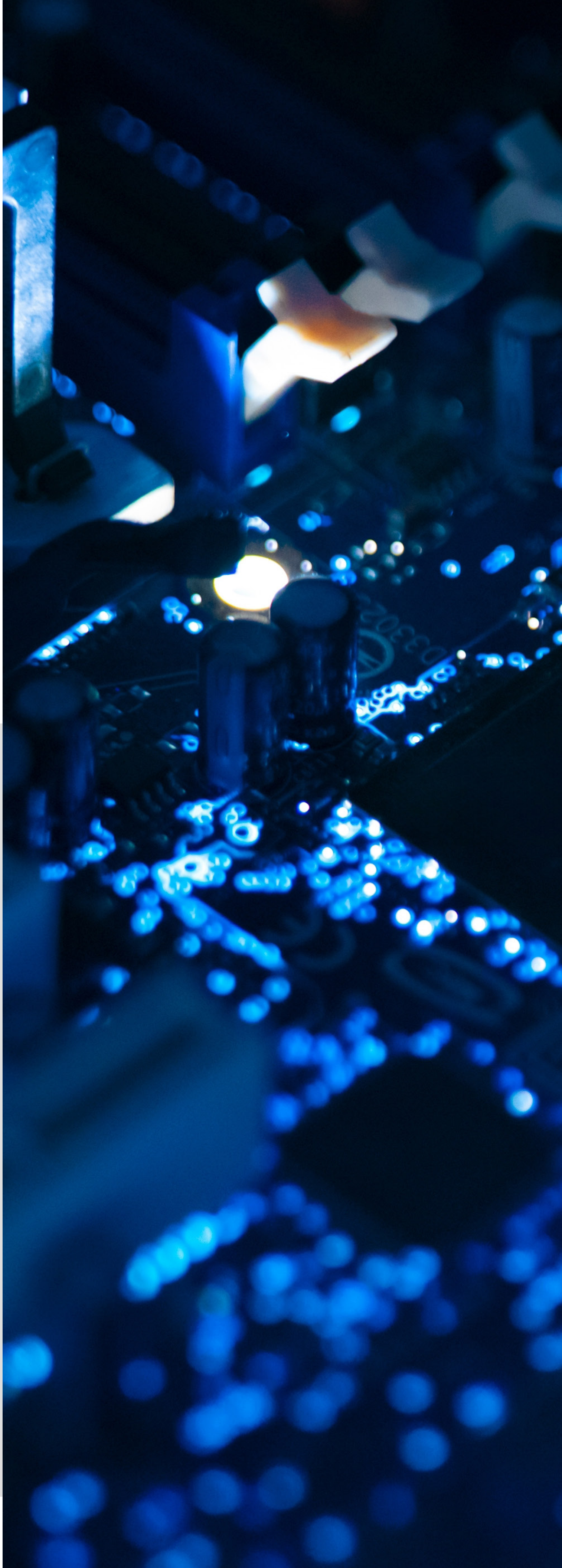
Findings from our 2025 Global Digital Trust Insights survey indicate that **hack-and-leak operations, third-party breaches, and cloud-related threats are the top cyber concerns for organisations in the Middle East.** These threats pose significant risks to brand reputation, regulatory compliance, and can result in significant financial losses and disruption.

Over the past three years, 15% of organisations in the region reported that their most damaging data breach cost their business more than US$100,000, while 13% estimated the cost of data breaches to be more than US$1million, emphasising the importance of robust cybersecurity measures to mitigate such risks. Global average data breach cost has exceeded US$3 million.

Thinking about the most damaging data breach your organisation experienced in the past three years, please provide an estimate of the cost.

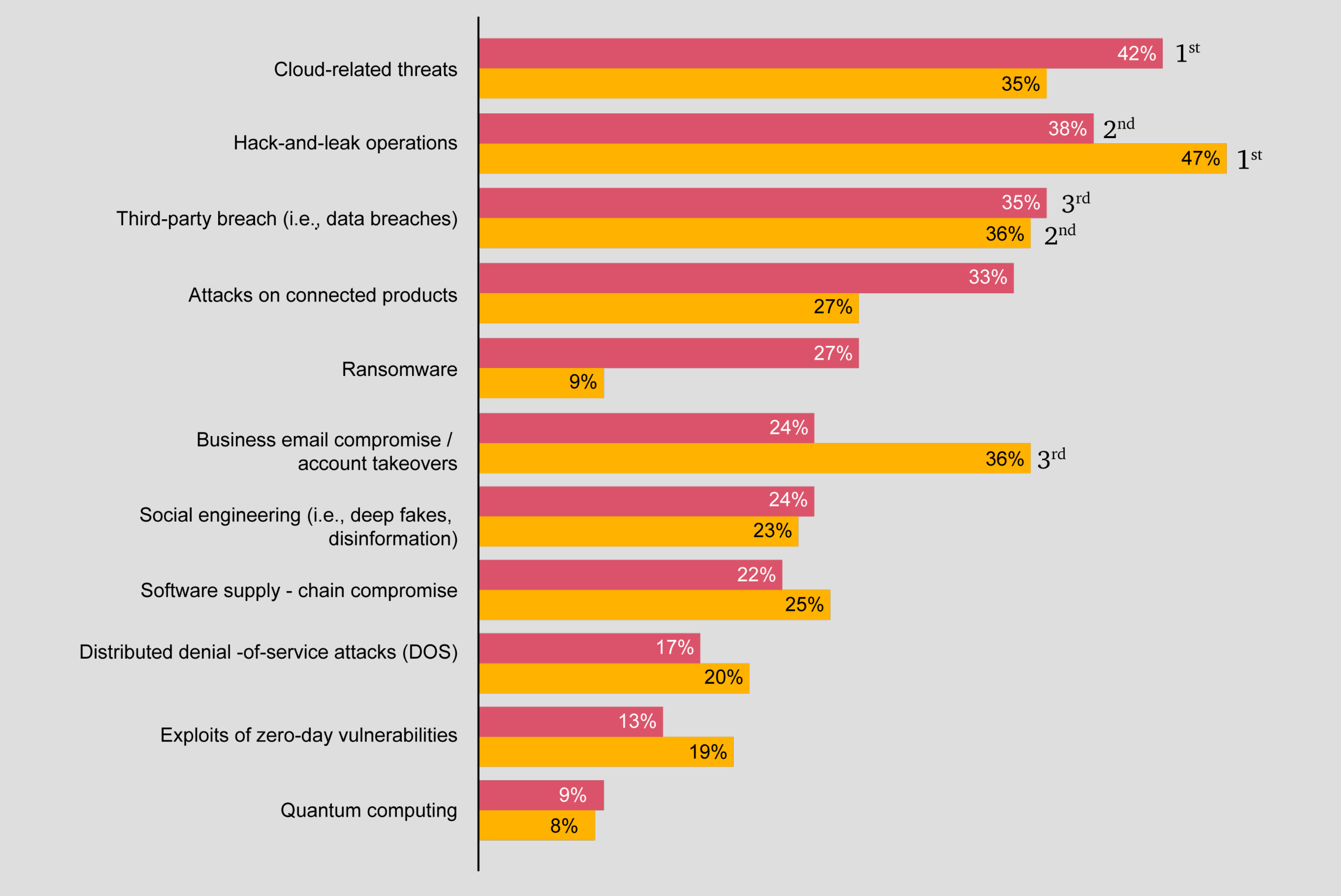


Source: PwC's Digital Trust Insights Survey, Final Results, August 2024.



In the Middle East, 47% of respondents were concerned over hack-and-leak operations (vs 38% globally), while 36% were concerned over third-party breach (vs 35% globally) and an equal number over business email compromise or account takeovers (significantly higher than only 24% of their global counterparts) and 35% over cloud-related threats (less than 42% globally). The higher percentages of hack-and-leak operations, data breaches and business email compromises in the region indicate a lower level of cyber maturity, with 34% of regional respondents saying they were least prepared to address third-party breaches over the next 12 months, compared to 28% of global organisations.

Over the next 12 months, which of the following cyber threats is your organisation most concerned about (e.g., risk to your brand, loss of business or business disruption, compliance)?



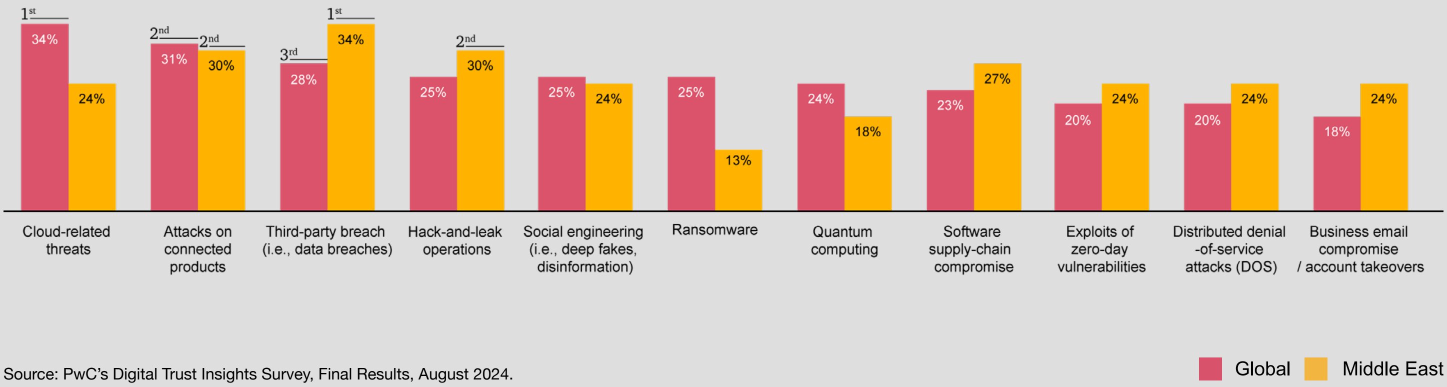
Source: PwC's Digital Trust Insights Survey, Final Results, August 2024.

Over the past few years, the region has been experiencing a significant increase in phishing attacks and smishing attacks. In the UAE, 92% of organisations surveyed by cybersecurity firm Proofpoint reported at least one successful phishing attack in 2023, up from 86% in 2022[5].

In the Digital Trust Insights Survey, 24% of respondents in the region – nearly a quarter of respondents – have indicated that their organisations were least prepared to address cloud-related threats over the next 12 months, compared to a sizeable 34% of their counterparts globally. This suggests that the Middle East is more proactive in cloud preparedness, driven by the rapid adoption of cloud technologies to transform the region's digital landscape.

Organisations in the region are leveraging cloud solutions to fuel growth and remain competitive in a fast-evolving world. According to the Cloud computing in the Middle East report, nearly a third (32%) have already starting implementing cloud in at least one area of their operations – while more than two thirds of respondents (68%) plan to migrate the majority of their operations to the cloud by mid-2025[6].

Over the next 12 months, which cyber threats do you think your organisation is least prepared to address?



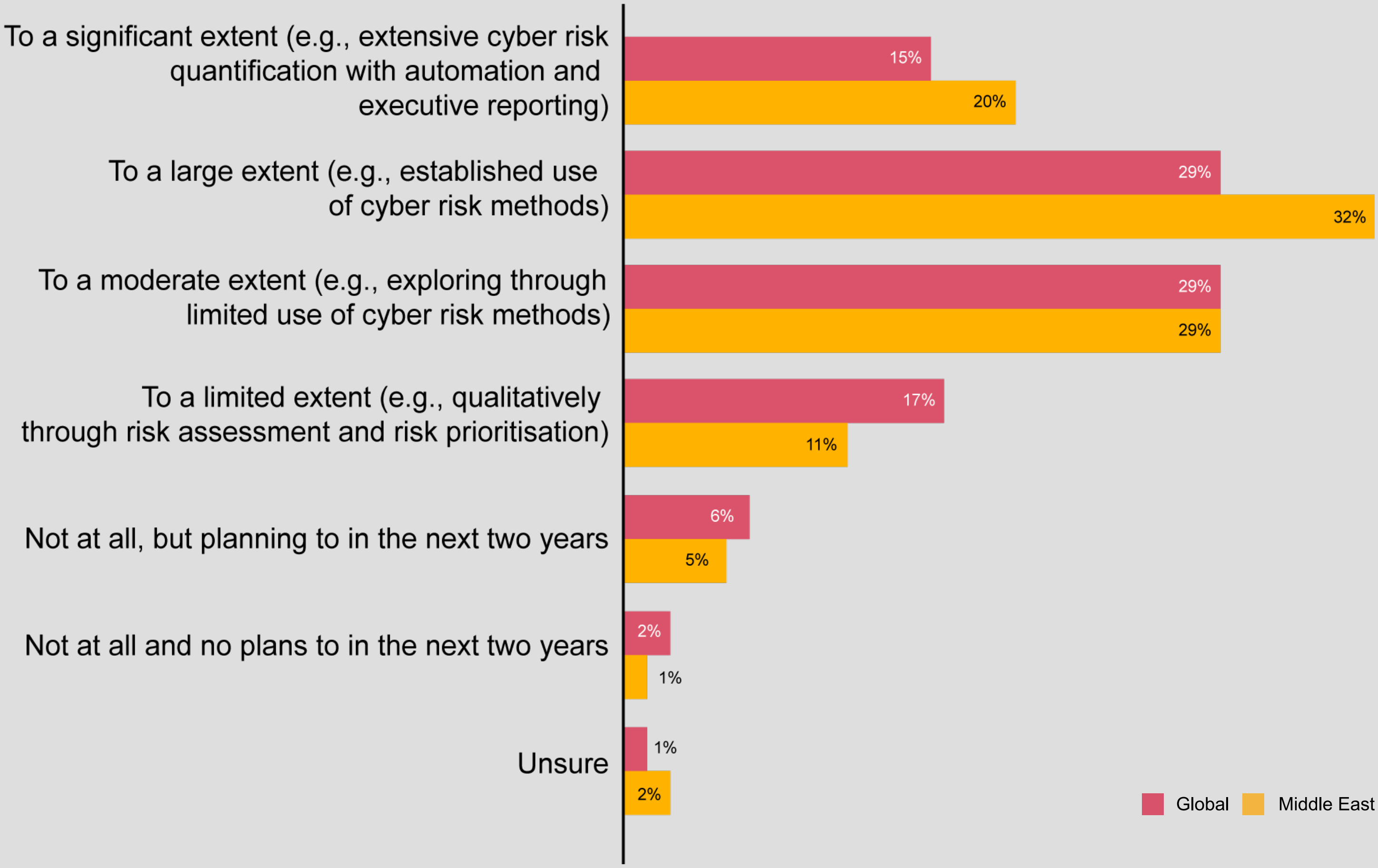
Source: PwC's Digital Trust Insights Survey, Final Results, August 2024.

Countries such as Saudi Arabia and the UAE have been instrumental in this shift, enacting legislation that mandates specific categories of data be stored within national borders[7]. This has led to the establishment of local data centres powered by the cloud, enabling businesses to meet compliance requirements while benefiting from enhanced security and operational efficiency.

Quantifying risks

When asked about their approach to quantifying the financial impact of cyber risks, more than half (52%) of regional organisations reported that they had largely or significantly established the use of cyber risk quantification methods, including employing automated risk quantification and executive reporting. This is 8% higher than the global average of 44%, indicating the seriousness Middle Eastern leaders place on safeguarding their company's bottom line from cyber threats.

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

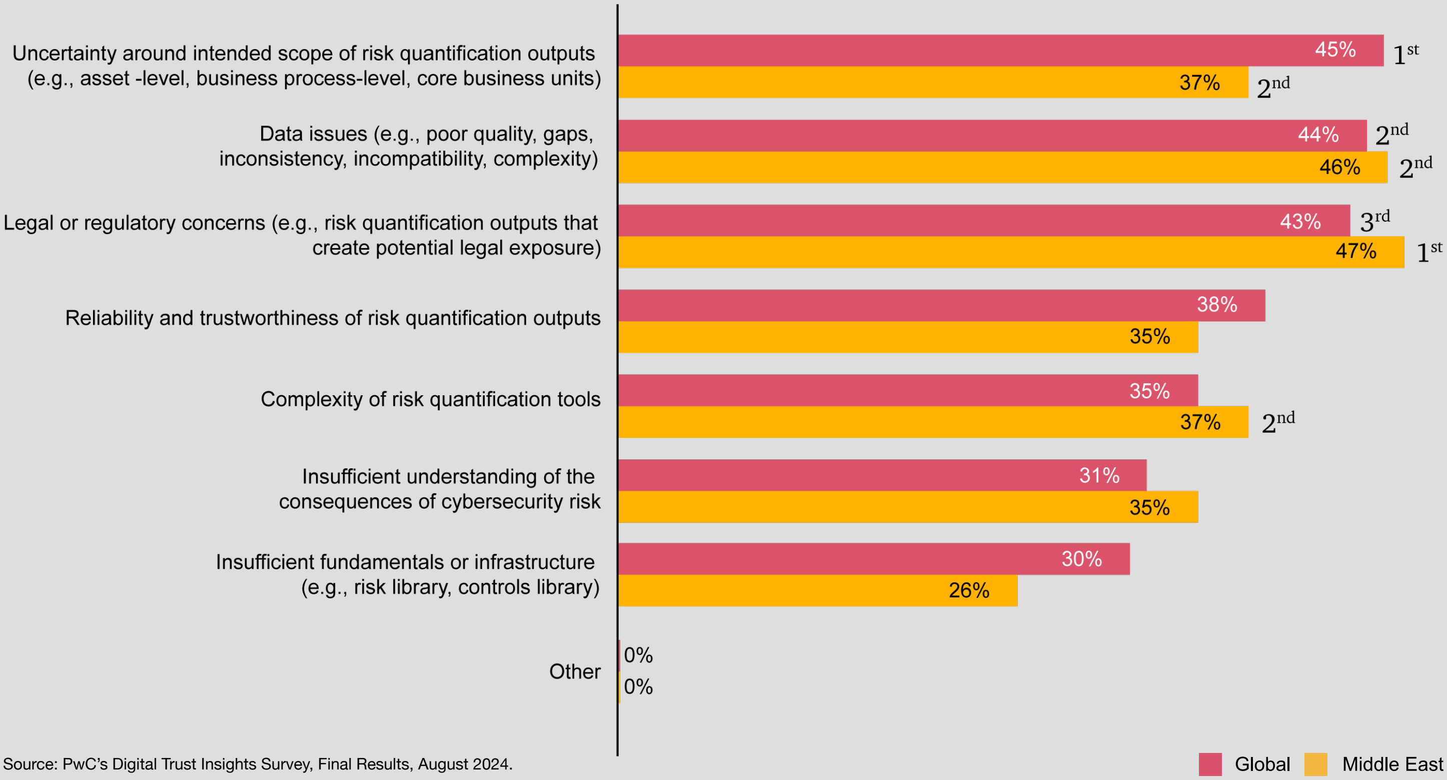


Source: PwC's Digital Trust Insights Survey, Final Results, August 2024.

Furthermore, when quantifying cyber risk, regionally, 69% of businesses rely on security posture assessments to measure compliance in areas such as vulnerability remediation, user access reviews, and staff training to strengthen their cyber risk evaluations.

However, challenges remain, with 47% highlighting legal or regulatory concerns, 46% indicating data issues, and 37% mentioning uncertainty around the intended scope of risk quantification outputs – indicating they were unsure of the purpose of the data generated through risk quantification. These sentiments were similar to those of their global counterparts.

What challenges, if any, has your organisation faced in quantifying the potential financial impact of cyber risk?



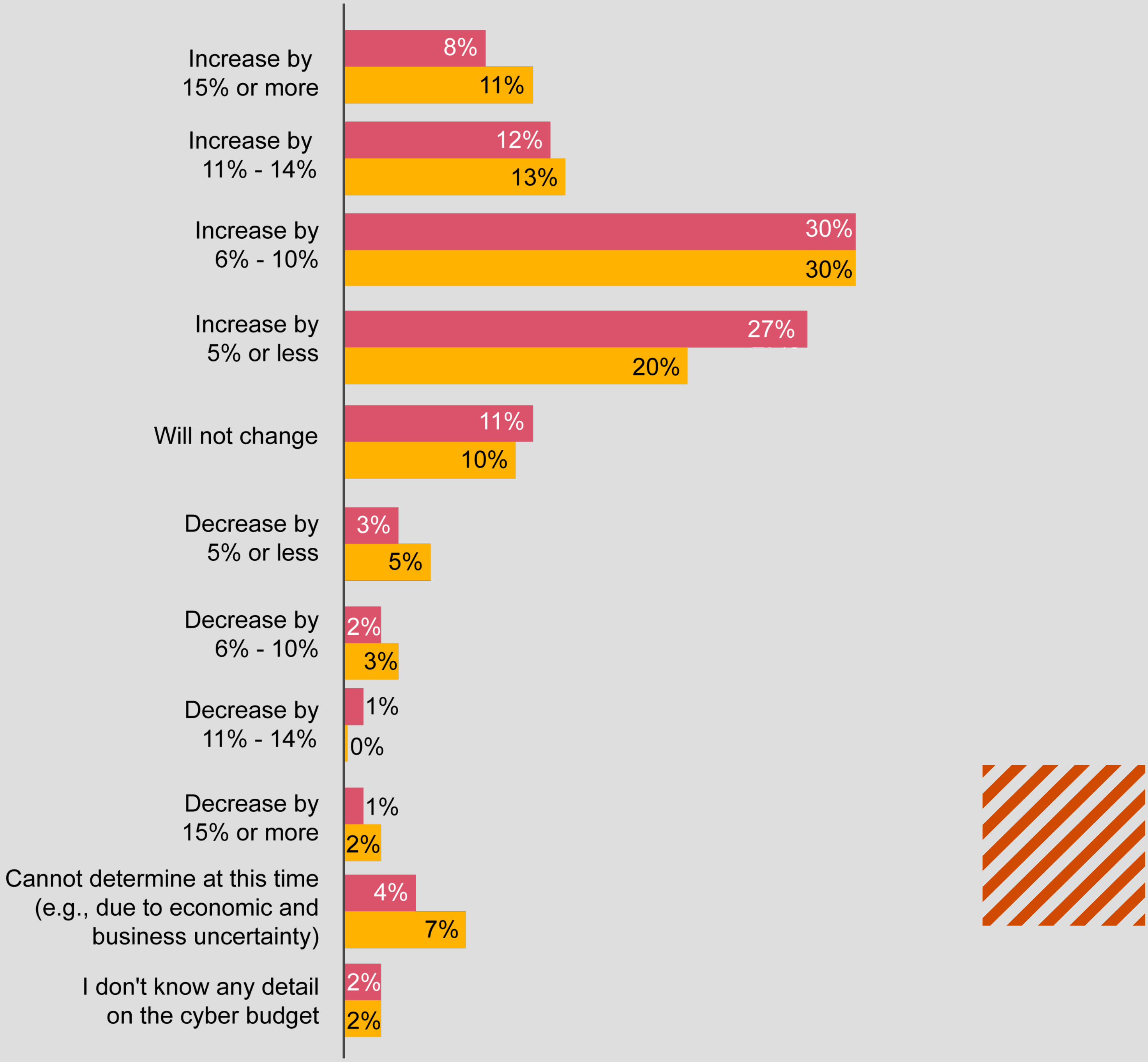
Source: PwC's Digital Trust Insights Survey, Final Results, August 2024.

Aligning cyber and business agendas:

Middle Eastern business and tech leaders focus on strategy and data protection

Nearly a quarter of Middle Eastern organisations plan to increase cyber budgets by at least 11% in 2025, compared to 20% globally, the 2025 Digital Trust Insights survey reveals interesting differences in investment priorities between business and tech leaders in the region.

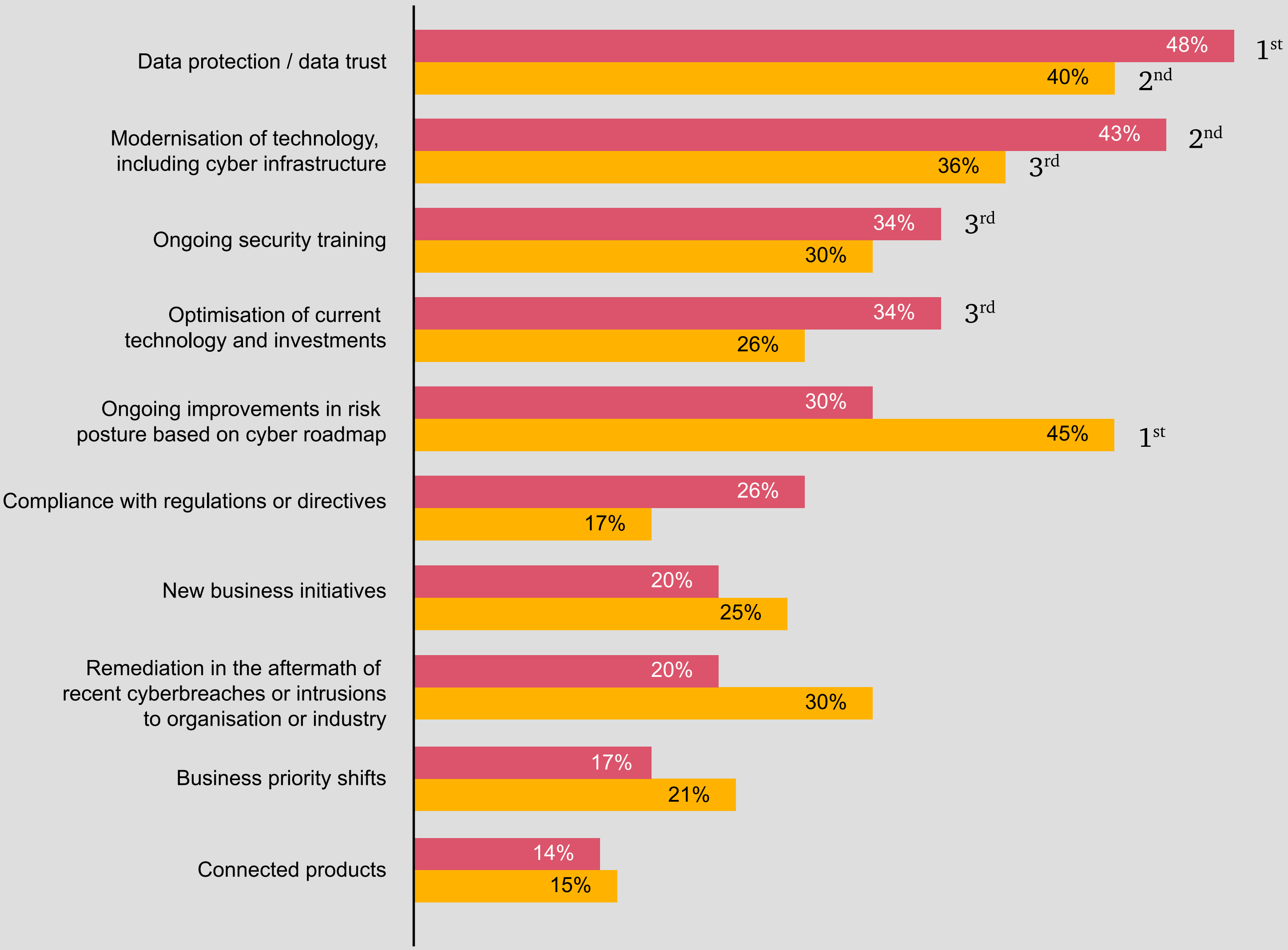
How will your organisation's cyber budget change in 2025?



Source: PwC's Digital Trust Insights Survey, Final Results, August 2024.

In the region, 45% of business leaders identified improving their organisation's risk posture, following a strategic plan, as their top investment priority (vs 30% globally), followed by 40% prioritising data protection (lower than 48% globally) and 36% focusing on modernisation of technology and cyber infrastructure (vs 43% globally).

Which of the following investments, if any, are you prioritising when allocating your organisation's cyber budget in the next 12 months?

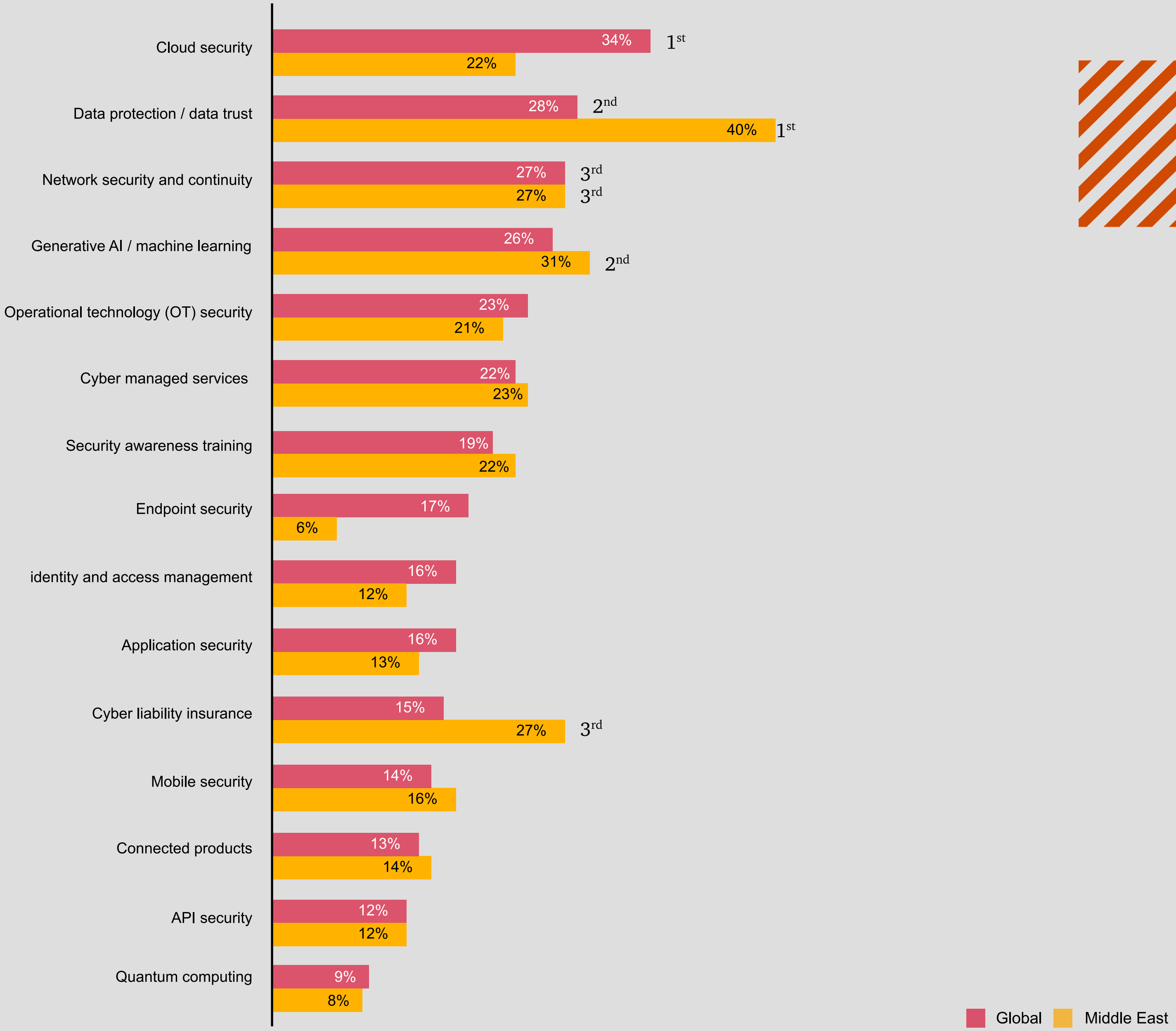


Source: PwC's Digital Trust Insights Survey, Final Results, August 2024.

🟥 Global 🟨 Middle East

For technology leaders, data protection, GenAI, and machine learning are top investment priorities. A sizeable 40% of regional technology leaders have data protection as their top investment priority, significantly higher than 28% of their global counterparts, followed by 31% prioritising GenAI and machine learning as a critical investment area, higher than 26% of their global counterparts.

Which of the following investments, if any, are you prioritising when allocating your organisation's cyber budget in the next 12 months?



Source: PwC's Digital Trust Insights Survey, Final Results, August 2024.

Despite differences in priorities, CISOs have an opportunity to collaborate with CEOs and align the cyber agenda with the business agenda. This will enable organisations to develop a well-rounded approach that addresses both immediate vulnerabilities and future challenges.

While the Middle East is undergoing rapid modernisation, there is an ongoing need to enhance cybersecurity measures to match this progress and safeguard critical infrastructure. For instance, malware detections in the UAE increased by 12% between January and May 2024, a trend reflected across Europe, the Middle East, and Africa, as highlighted in a July report by Swiss cybersecurity firm Acronis[5].

In the wider region, the asset-heavy energy and utilities sectors have cybersecurity integrated into their operations and maintenance budgets. However, as the threat landscape evolves and cyberattacks become more frequent, these organisations, followed closely by the banking and financial services sector as well as telecommunications and retail, must continuously increase their cybersecurity spending to safeguard their infrastructure.

Findings from our last year's survey had also indicated the need for organisations to optimise existing technologies and investments - more than half (53%) of our regional respondents identified it as highest potential to create value, while 43% selected technology modernisation, including cyber infrastructure.

Middle East CEOs, CISOs, and Boards in sync

In the Middle East there is a significant emphasis on cybersecurity and privacy at both executive and board levels, with greater involvement from leadership compared to global counterparts.

- **41% of regional respondents reported that their CEOs were involved in discussions about the cyber and privacy implications of new business initiatives, higher than their global counterparts. Findings also reveal that CEOs discussed cyber and privacy concerns for future corporate strategies, major operating model changes, as well as deal making.**
- **A significant 61% indicated that their CISOs were involved to a large extend in strategic planning with CFOs about cyber investment, higher than 47% globally. More than half revealed that CISOs also had regular meetings with the board, compared to 46% globally. An equal percentage said the CISO had oversight on tech and infrastructure deployment, higher than 45% globally.**
- **At the highest level, the board, 50% agreed that the board was very effectively involved in cyber strategy, higher than 47% globally. More than half also said the board had a cyber risk oversight, compared to 46% globally.**

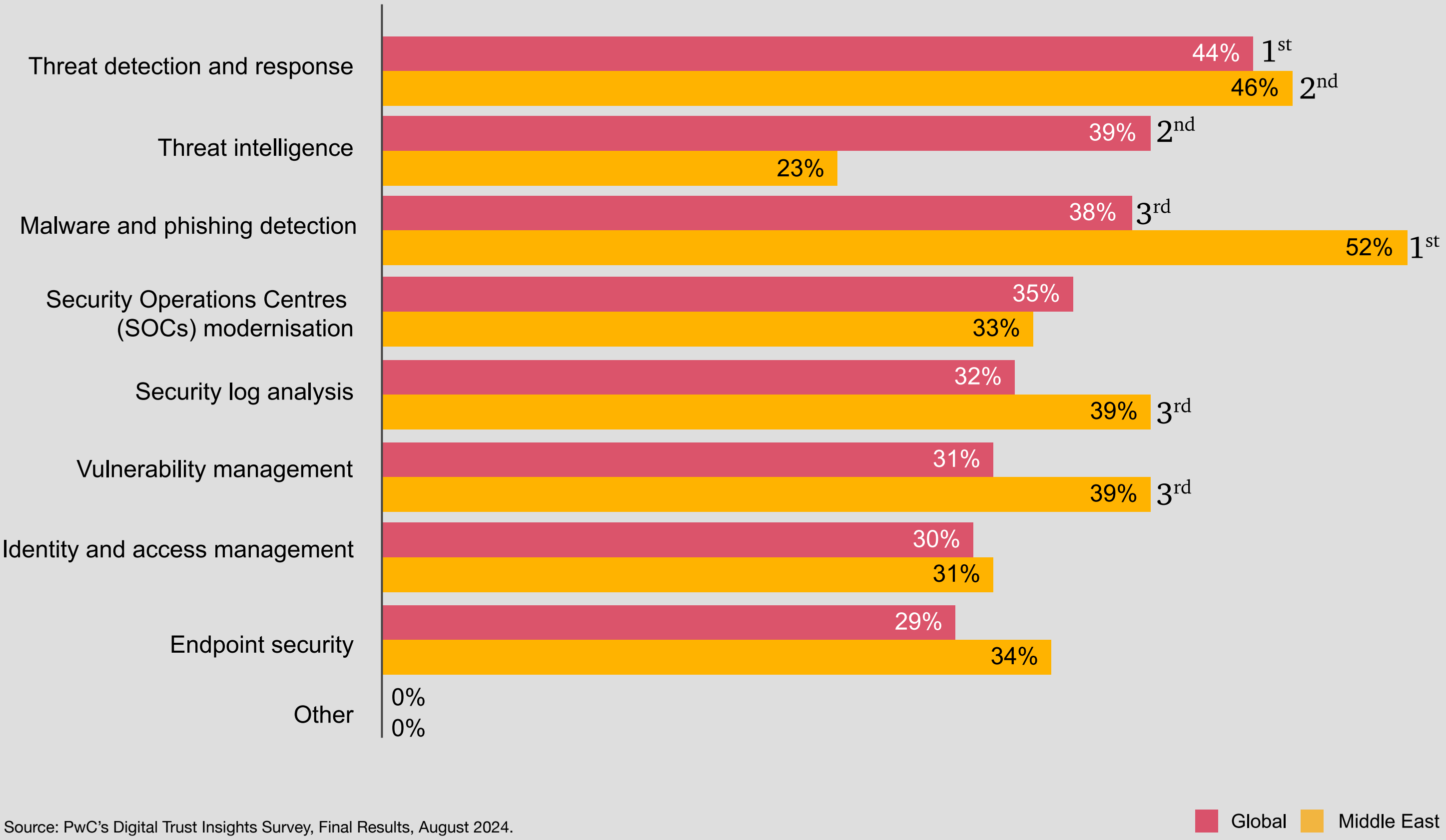
The strong involvement of CEOs, CISOs, and Boards in Middle Eastern organisations reflects a proactive approach to integrating cybersecurity into strategic planning, making them more resilient to evolving threats. Additionally, the collaboration between CISOs, CFOs, and boards fosters a holistic approach, aligning financial, technical, and risk management perspectives, resulting in better budgeting, strategic investments, and faster technology adoption.

Organisations look to GenAI and emerging technologies to continue strengthening cyber defence

At a time of heightened cybersecurity concerns in the Middle East, tech leaders are anticipating GenAI's positive impact on cyber defence. In our Middle East GenAI spotlight, a significant 83% of Middle East respondents (including 92% in the UAE and 87% in the KSA) had revealed that their organisations would deploy GenAI tools for cyber defence within the next 12 months, compared to 69% globally[6]. GenAI has the power to unify data from diverse sources, enabling organisation to rapidly identify vulnerabilities, prioritise critical actions, and gain a comprehensive view of the entire attack surface. This capability can enhances decision-making processes, and strengthens proactive defenses against emerging threats.

As a result, GenAI is rapidly gaining momentum as a key tool in cyber defense across the Middle East. Our latest survey respondents in the region have prioritised it for malware and phishing detection (52%), threat detection and response (46%), security log analysis, and vulnerability management (both at 39%) over the next 12 months. Fraud detection has emerged as a key use case for GenAI in the Middle East's financial services sector[7].

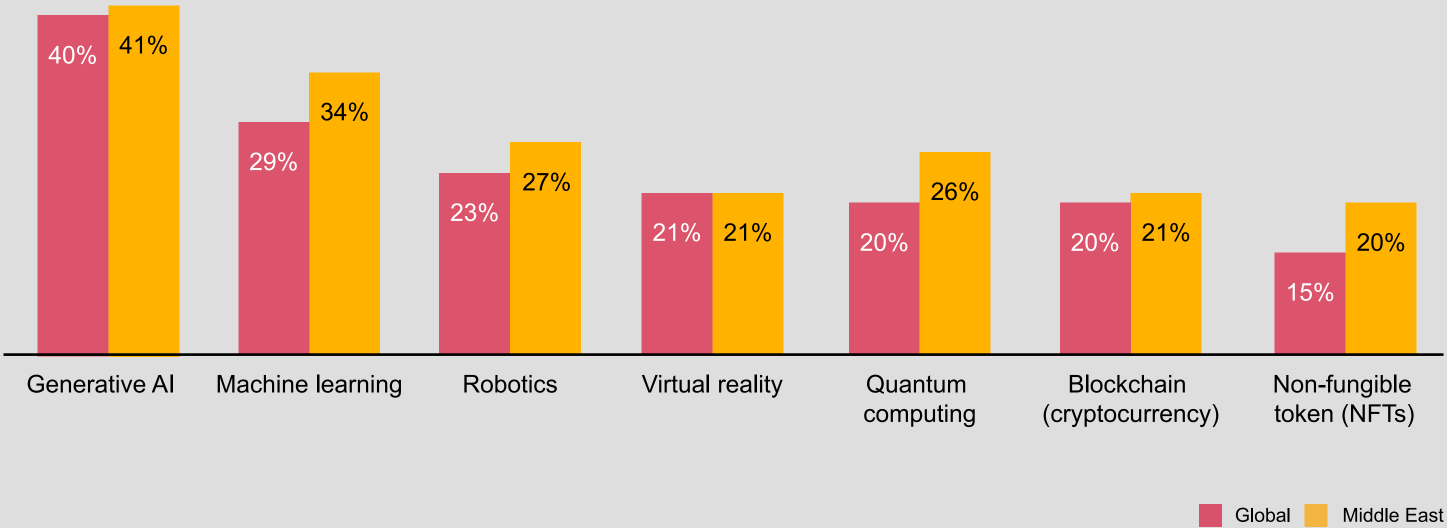
In what aspects of cyber defence, if any, is your organisation prioritising the use of generative AI (GenAI) over the next 12 months?



Source: PwC's Digital Trust Insights Survey, Final Results, August 2024.

Findings of our latest survey have also highlighted that 41% of regional respondents reported a significant increase in GenAI investments over the past 12 months, closely aligned with global (40%). This was followed by investments in machine learning (34%) and robotics (27%).

To what extent has your cyber investment changed, if at all, for these emerging technologies in the past 12 months?



Source: PwC's Digital Trust Insights Survey, Final Results, August 2024.

This mirrors the sentiment in our 27th Annual CEO survey: Middle East findings, where 73% of regional CEOs are optimistic about the potential impact of GenAI, believing that it will significantly change the way their company creates, delivers and captures value in the next three years[8]. However, 33% of regional respondents to our latest digital trust survey also reported that GenAI had significantly expanded the cyber-attack surface in their IT environment over the past year, with cloud technology identified as the next major contributor. With 68% of Middle Eastern companies planning to migrate their operations to the cloud within the next two years[9], the expansion of cloud technology has significantly increased the cyber-attack surface. Cloud services are playing a pivotal role in the region's ongoing national transformation initiatives, digitisation of services, and data localisation drive[10], particularly with the emergence of sovereign clouds[11].

GenAI, opportunities and challenges

In relation to cybersecurity and privacy, more than half of respondents indicated that their organisations are likely to face challenges integrating GenAI with existing systems and processes. Another 48% highlighted the potential risk of an employee deliberately misusing GenAI technology – which explains the 28% of respondents who said GenAI had significantly increased organisational risk management investments in talent hiring and training.

Further challenges include inadequate internal controls and risk management, the inability to comply with new regulations, and a lack of training resources for employees. Additionally, 30% also pointed to a lack of trust in GenAI among leadership and employees as a significant hurdle. This underscores the importance of building confidence through proper training and clear communication about the benefits and risks of GenAI in the workplace. Without addressing these issues, the full potential of GenAI in enhancing cybersecurity may not be realised.

Is blockchain expansion boosting cyber risk?

Another emerging technology that has significantly increased the Middle East's cyber-attack surface is the blockchain, cited by 30% of regional respondents, versus just 17% globally. The vast difference between regional and global figures could be attributed to the higher-than-average financial sector use cases for blockchain in the Middle East, with the UAE[12], Bahrain[13], and Saudi Arabia[14] all deploying cryptocurrency-based solutions. The larger attack surface has also significantly increased cyber investment towards blockchain in the past 12 months for 21% of respondents, similar to their peers globally.

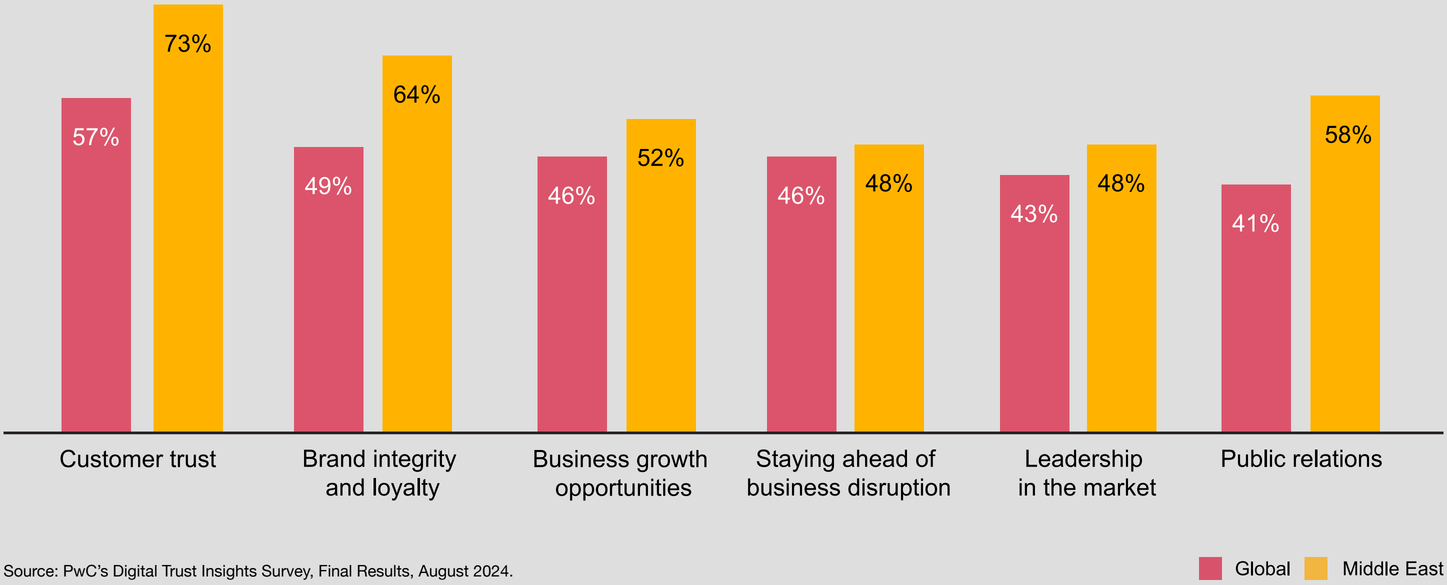
Cyber investment in quantum has the largest investment differentiation, where the trend is 6% over the global budget changes, to address such cybersecurity concerns in the past 12 months. Middle East organisation have prioritised this risk likely on the basis of the global trend to address quantum and releasing of directives from US and EU, along with NIST guidance. This is despite local Middle East regulation to address post quantum cryptography and its transition from legacy encryption to the new approved algorithms. Showing a good understanding of the risk and expected prolonged transition from legacy cryptography in complex digital environments.

Building cyber resilience: A strategic approach to growth and security

Cyber resilience is a critical strategy for organisations to protect its digital assets. It acknowledges that no system, regardless of its strength, is immune to vulnerabilities and focuses on an organisation's ability to sustain core operations not only during a cyberattack but also throughout the recovery process.

In the Middle East, organisations increasingly view cybersecurity as a strategic asset, positioning it as a competitive advantage to build customer trust (73% vs 57% globally), drive brand integrity and loyalty (64% vs 49% globally) and strengthen business growth opportunities (52% vs 46% globally) to a large extent.

To what extent does your organisation position cybersecurity as a competitive advantage in these areas?



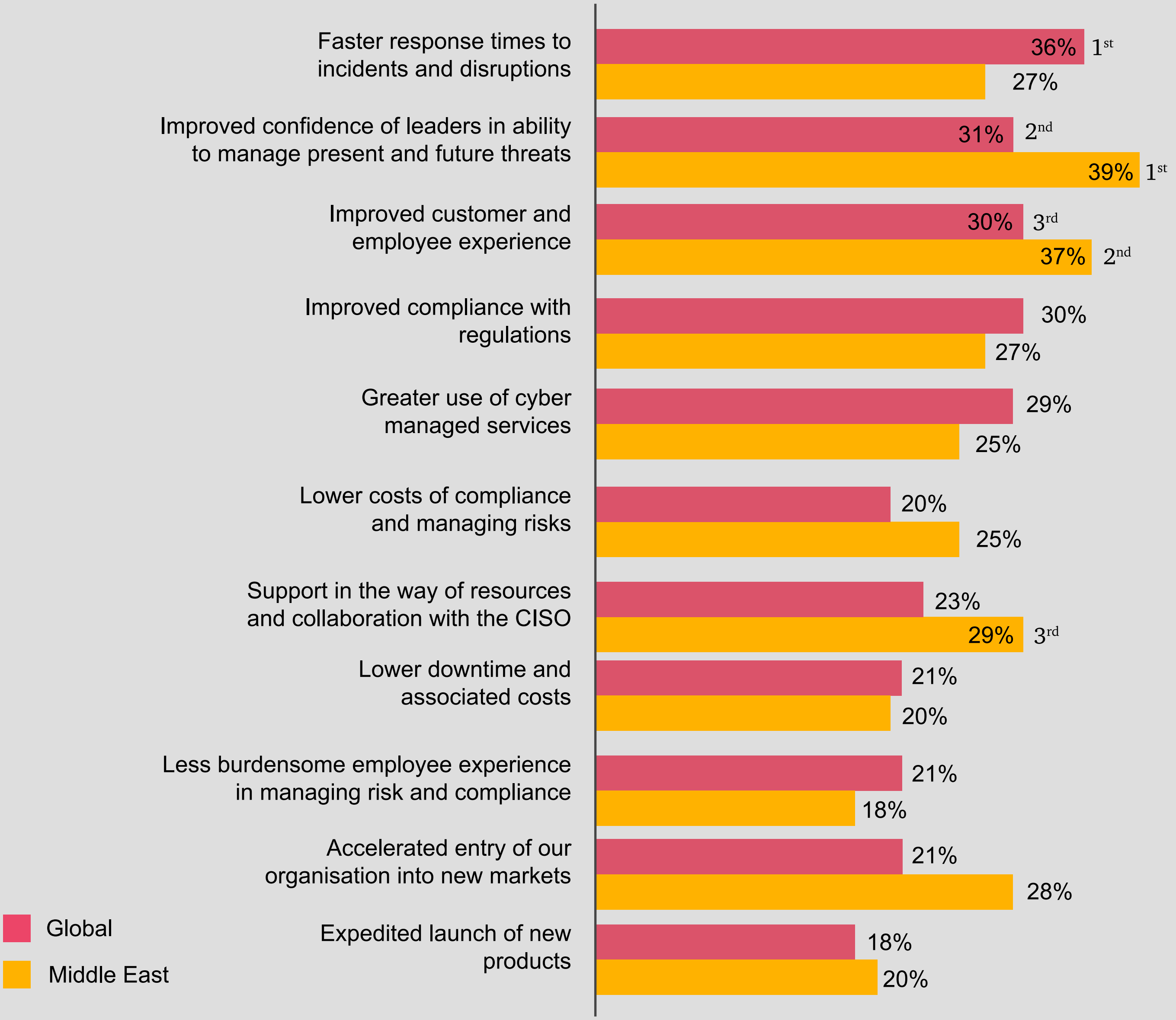
Source: PwC's Digital Trust Insights Survey, Final Results, August 2024.

This strong focus on cybersecurity is further reinforced by proactive measures taken to strengthen resilience across their operations. 41% of regional respondents (compared to 34% globally) have already established a resilience team across their organisations, with members from business continuity, cyber, crisis and risk management. Furthermore, 42% of regional respondents indicated that they were currently implementing cyber recovery technology solutions in parts of their organisations and 32% were planning to deploy quantum computing for cyber defence and resilience over the next two years.

When revealing their organisation's strategy, people, and investment goals related to cyber and privacy over the next 12 months, 39% of regional respondents prioritised improving leaders' confidence in managing current and future threats. Additionally, 37% focused on enhancing customer and employee experience, while 29% emphasised collaboration with the CISO and increased resource support. These priorities are largely in line with global peers.

However, a notable difference emerged regarding incident response times. Only 27% of regional respondents highlighted faster response to incidents and disruptions as a key strategy compared to 36% globally. The disparity with global counterparts suggests that regional firms may need to place greater emphasis on speed and efficiency in addressing cyber threats to mitigate risks and minimise disruption. Faster response times are crucial for reducing the impact of breaches and ensuring business continuity in a rapidly evolving threat landscape.

What, if any, are your organisation's strategy, people, and investment goals relating to cyber and privacy over the next 12 months?



Source: PwC's Digital Trust Insights Survey, Final Results, August 2024

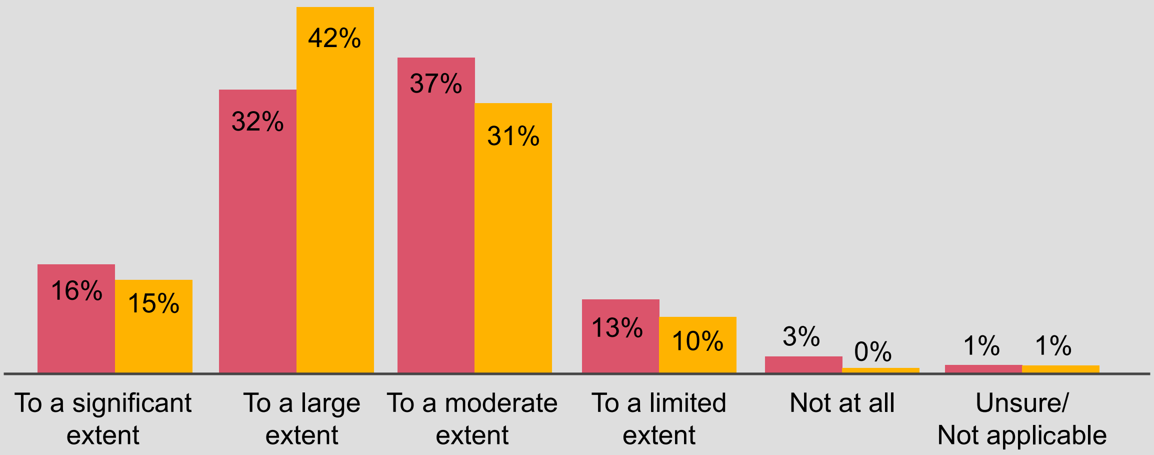
Regulation and leadership: Driving cybersecurity resilience through robust governance

Given the increasing speed in which cyber attackers are now exploiting security vulnerabilities, compliance with evolving cybersecurity regulations is a top priority for Middle Eastern organisations. In our latest survey regional respondents have shown a greater confidence (extremely and very confident) in their organisation's ability to comply with regulations related to data protection (72%), consumer privacy (68%) and network and information security (68%), than their global counterparts. Findings have also revealed that a quarter of respondents regionally (25%) expressed only moderate confidence in their organisation's ability to comply with AI- and resilience-related regulations, implying that more needs to be done in this area.

Even though organisations in the Middle East comply with several international regulations, such as the EU General Data Protection Regulation (GDPR), countries in the region have their own regulatory framework to raise the security levels of service providers. Communications, Space & Technology Commission in KSA, for example has implemented a regulatory framework for service providers in the communications, IT, and postal (services) sector[15], while in the UAE, the Cybersecurity Council is currently working on developing three new policies to be issued by the end of 2024[16] around "cloud computing and data security", "Internet of Things security", and "cybersecurity operations centres".

Cybersecurity regulations have largely or significantly driven cybersecurity investment for 57% of Middle Eastern respondents (vs 46% globally), with 21% specifically crediting new regulations for enhancing their organisation's resilience by enforcing an industry-wide framework.

Which of the following risks is your organisation prioritising for migration over the next 12 months?



Source: PwC's Digital Trust Insights Survey, Final Results, August 2024

Interestingly, there is a distinct approach to regulatory responsibilities among leadership in the Middle East, compared to global counterparts. While Middle Eastern CEOs are less directly involved in regulatory actions (33% vs 36% globally), there is stronger involvement from Chief Information Security Officers (CISOs), with 46% of regional respondents indicating that their CISO takes a lead role in drafting and reviewing regulatory disclosures – 5% higher than the global average.

The most notable leadership difference lies at the board level, where 63% of Middle Eastern respondents believe their board is highly effective in executing regulatory responsibilities, significantly surpassing the global average of 50%. This suggests that in the Middle East, regulatory responsibilities are more concentrated at the board and CISO levels, indicating a strong governance framework.

Actionable insights for leaders:

As the region undergoes rapid digital transformation, decision-makers must embed cybersecurity into every strategic decision to safeguard growth and innovation.

Only 39% of Middle Eastern CEOs are currently involved in discussions on the cyber and privacy implications of future corporate strategies. Business leaders should be more involved in aligning future strategies with evolving compliance requirements.

With the region's focus on public cloud growth, leaders also need to allocate more budget to address cloud-related threats. The growing adoption of cloud services requires increased investment to mitigate cyber risks effectively.

As part of organisation behaviour and culture, leaders must encourage proactive collaboration. Currently, only 27% of respondents say their cybersecurity teams regularly implement controls and respond swiftly to threats, implying that there is an opportunity for other organisations to speed up their response time.

Additionally, only 17% of respondents reported that their cybersecurity teams collaborate with other departments, indicating the need to increase this collaboration to enhance the security postures of substantially higher number of businesses.

To avoid a siloed approach that weakens the overall security posture, cybersecurity must be integrated across all business functions. Leaders must encourage collaboration between cybersecurity teams and other departments will improve response times and risk management.

Furthermore, with growing importance of AI, it is crucial to establish a common framework in the region regulating AI-related activities to strengthen market confidence and attract tech investments. As we have explored in our report GenAI: Who draws the ethical line, business leaders need to collaborate with government entities, regulatory bodies, and industry peers to foster the development of effective, resilient regulations that address the challenges brought by AI[17]. This is essential for creating a framework that not only upholds ethical values and societal norms but also fosters innovation and technological progress in the region.

Contact us

Samer Omar
Cybersecurity and Digital Trust Leader
PwC Middle East
samer.omar@pwc.com | LinkedIn

Clinton Firth
Cybersecurity and Digital Trust Partner
PwC Middle East
clinton.firth@pwc.com | LinkedIn

Raddad Ayoub
Cybersecurity and Digital Trust Partner
PwC Middle East
raddad.ayoub@pwc.com | LinkedIn

Fady Chalhoub
Cybersecurity and Digital Trust Partner
PwC Middle East
fady.chalhoub@pwc.com | LinkedIn

Haitham Al-Jowhari
Cybersecurity Partner
PwC Middle East
haitham.al-jowhari@pwc.com | LinkedIn

Hemant Arora
Cybersecurity and Digital Trust Partner
PwC Middle East
hemant.a.arora@pwc.com | LinkedIn