pwc

New world, new rules: Cybersecurity in an era of uncertainty

2026 Global Digital Trust Insights: C-suite playbook and findings

60%

are increasing cyber risk investment in response to geopolitical volatility

Only 6%

have fully implemented all data risk measures surveyed

Top 2

challenges to implementing AI for cyber defence are knowledge and skills gaps

Cybersecurity is entering uncharted waters. A rapidly shifting world order and threat environment — powered by recent, exponential leaps in technology — is putting cyber strategies to the test.

Organisations are confronting the new reality of a post-globalisation era, one that's marked by fractured alliances, weakened global institutions, tariff shocks and disrupted supply chains. We're witnessing unprecedented technology advances that are expanding the attack surface and introducing novel cyber threats, many of them state-sponsored.

All this uncertainty is forcing executives to reassess their capabilities, talent and technology. More fundamentally, it's forcing them to revisit their cyber strategy, including where they operate and whom they do business with.

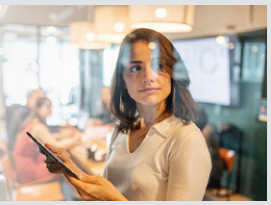
PwC's 2026 Global Digital Trust Insights survey of 3,887 business and tech executives across 72 countries reveals how leaders are handling this era of uncertainty, where they're falling short and what they might do differently to better meet the challenge. Among the key findings:

- **Geopolitical risk is shaping strategy:** 60% of business and tech leaders rank cyber risk investment in their top three strategic priorities in response to ongoing geopolitical uncertainty.
- **Resilience is a work in progress:** Given the current geopolitical landscape, roughly half say their organisation is at best only 'somewhat capable' of withstanding cyber attacks targeting specific vulnerabilities. Only 6% feel confident across all vulnerabilities surveyed.
- **Waiting for trouble:** Only 24% of organisations are spending significantly more on proactive measures (e.g., monitoring, assessments, testing, controls) than reactive measures (incident response, fines, recovery). That's the ideal spend ratio. Most companies (67%) are spending roughly equal amounts on both categories, which can be more costly and risky.
- **AI agents for cyber defence:** Agentic AI ranks among the top AI security capabilities organisations are prioritising over the next 12 months. They plan to deploy these agents for cloud security, data protection and cyber defence and operations, among other priority areas.

- **The quantum clock is ticking:** Although quantum computing ranks among the top five threats organisations are least prepared to address, fewer than 10% prioritise it in budgets and only 3% have implemented all leading quantum-resistant measures surveyed.
- **Rethinking the cyber talent crisis:** Skills shortages remain one of the biggest barriers to cyber progress. Over half (53%) are prioritising AI and machine learning tools to help close capability gaps, and specialised managed services are becoming strategic accelerators to provide expertise and scale.

Meeting the moment will require renewed urgency, creativity and different approaches — not a business-as-usual mindset. Our C-suite playbook translates this year's findings into practical steps, helping key stakeholders strengthen their foundational security practices and implement future-ready measures calibrated to the evolving world we're in.

Table of contents



01

Risk and threat landscape

Geopolitics are reshaping cyber vulnerabilities

60%

are increasing cyber risk investment in response to geopolitical volatility

Only 6%

are 'very capable' of withstanding cyber attacks across all vulnerabilities surveyed given the geopolitical landscape

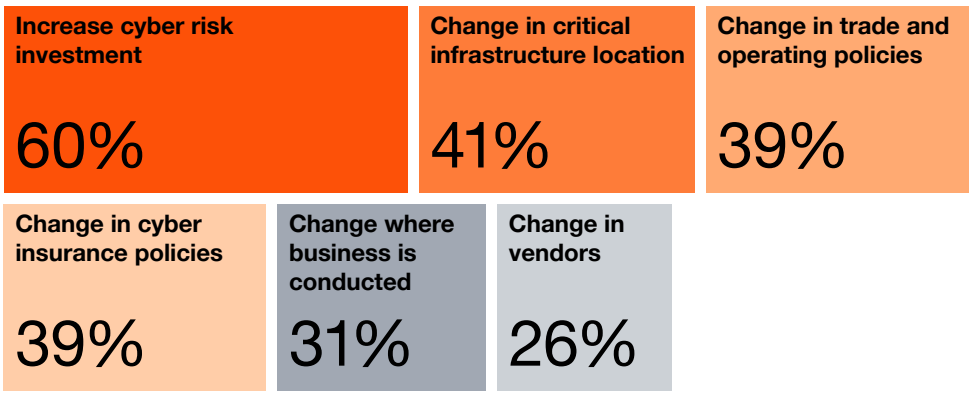
Top 2

cyber threats organisations are least prepared to address: cloud and connected product attacks

Today's cyber risks are shaped as much by geopolitics as by disruptive technologies. Upended alliances, trade disputes, weakened international institutions and other destabilising trends in this new era of strategic competition are reshaping the threat environment, as well as traditional methods of doing business.

Responding to this geopolitical climate, 60% of business and tech leaders are making cyber risk investment one of their top three strategic priorities for the year ahead. They're also prioritising changes in critical infrastructure location (41%), trade and operating policies (39%) and cyber insurance policies (39%). With disruption now the norm, cyber is a critical lever for resilience.

Cyber strategy changes in response to current geopolitical landscape
(% that ranked in their top 3 areas)

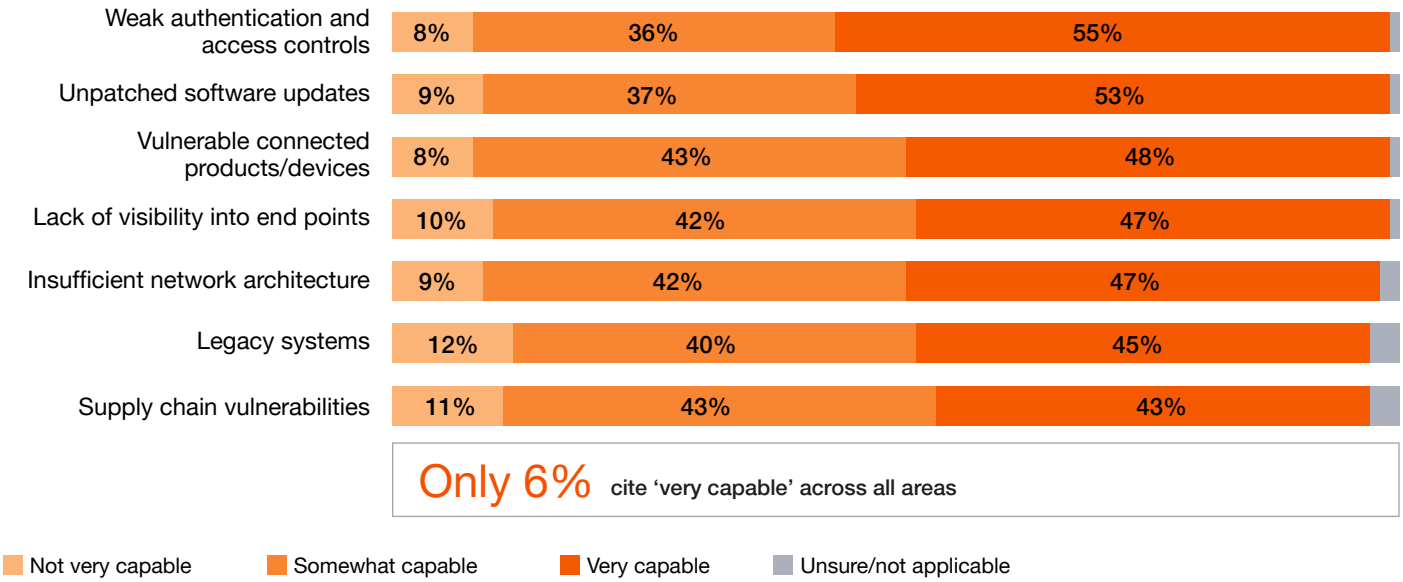


Q2. Over the next 12 months, which of the following areas of your organisation's cyber strategy is changing in response to the current geopolitical landscape? Base: All respondents=3887
Source: PwC 2026 Global Digital Trust Insights

Feeling secure vs being secure

Given the current geopolitical landscape, confidence in cyber readiness is split. While about half of respondents say their organisations are 'very capable' of withstanding cyber attacks targeting specific vulnerabilities surveyed, just as many aren't prepared. What's more, only 6% say they're very capable across all vulnerabilities surveyed. Legacy systems and supply chain exposures are among the weakest spots and remain frequent targets for nation-state actors aiming to disrupt critical infrastructure.

Capability to withstand a major cyber attack



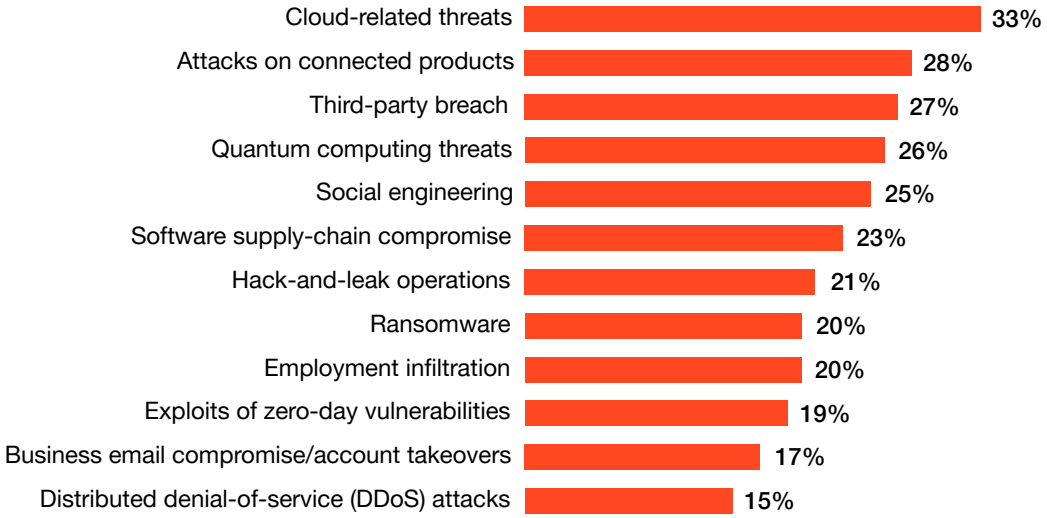
Q3. Given the current geopolitical landscape, how capable is your organisation to withstand a major cyber attack targeting the following vulnerabilities?
Base: Security leaders, COOs and Operations Directors=1971
Source: PwC 2026 Global Digital Trust Insights

Persistent gaps, rising stakes

Beyond the above vulnerabilities, leaders have concerns about their readiness for specific types of threats. Cloud and connected product attacks remain top concerns, similar to last year's findings, with roughly one-third of leaders ranking them in the top three cyber threats their organisation is least prepared to handle.

These risks aren't new, but with AI-enabled adversaries pushing the envelope, they reflect ongoing challenges in closing foundational gaps in governance, control and visibility. As technology and ecosystem complexity grows, many organisations are straining to keep pace, especially across third-party and supply chain dependencies.

Cyber threats organisations are least prepared to address
(% that ranked in their top 3 threats)



Q1. Over the next 12 months, which of these cyber threats is your organisation least prepared to address?
Base: Security leaders=1740
Source: PwC 2026 Global Digital Trust Insights

Learning the hard way

For several years now, more than a quarter of executives tell us their most damaging data breach in the past three years cost their organisation at least $1 million. The most exposed? Enterprises with $5 billion or more in revenue (41%), US-based companies (37%) and companies operating in the tech, media and telecom industry (33%). For them, the scale and complexity of operations raise the likelihood of high-cost incidents.

Given the challenges of recovery, organisations that have experienced a major attack are turning costly lessons learned into action. They're doing more than others to increase cyber budgets (88%, vs 78% overall) and embrace managed services to fill critical skills deficiencies (48%, vs 39% overall). They're also more likely to change cyber insurance policies (49%, vs 39% overall), possibly in response to rising premiums and insurer expectations. And many are embedding more data-minimisation practices across the organisation.

02

Cyber strategy and operations

Where investment meets impact

Only 24%

are spending significantly more on proactive vs reactive cybersecurity measures

78%

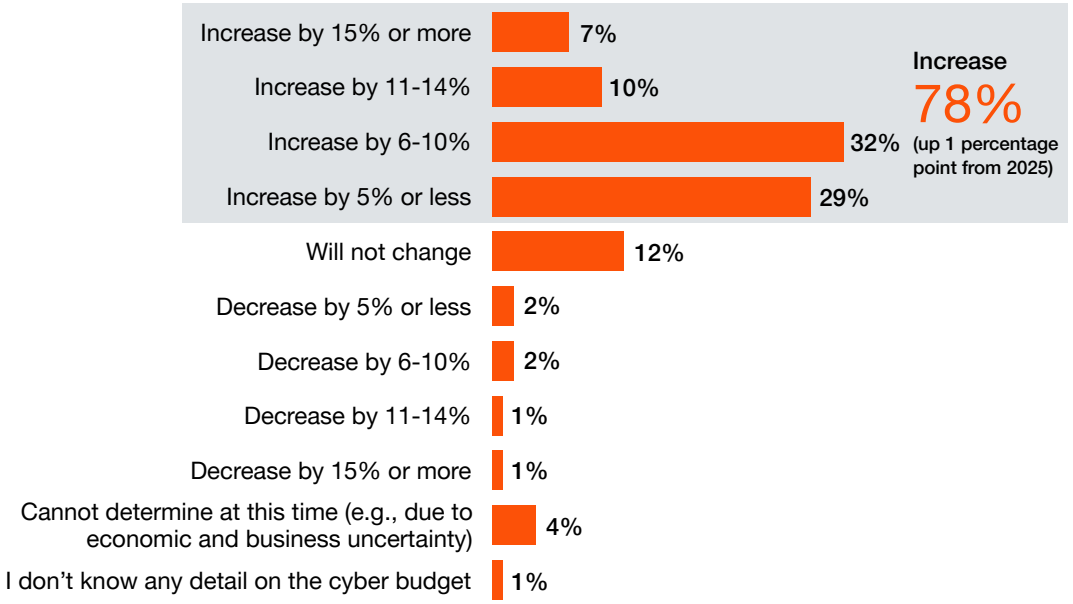
expect their cyber budget to increase over the coming year

Only 16%

are measuring the financial impact of cyber risks to a significant extent

Are cyber budgets keeping pace with the times? Nearly eight in ten (78%) say their cyber budget will increase over the coming year. But that's virtually unchanged from last year (77%). While respondents say they're increasing cyber risk investment in response to the current geopolitical landscape, it may be coming at the expense of other spending priorities.

Cyber budget change in 2026



Q8. How will your organisation's cyber budget change in 2026? Base: Security leaders, CFOs and Finance Directors=2027
Source: PwC 2026 Global Digital Trust Insights

The cost of preparing vs reacting

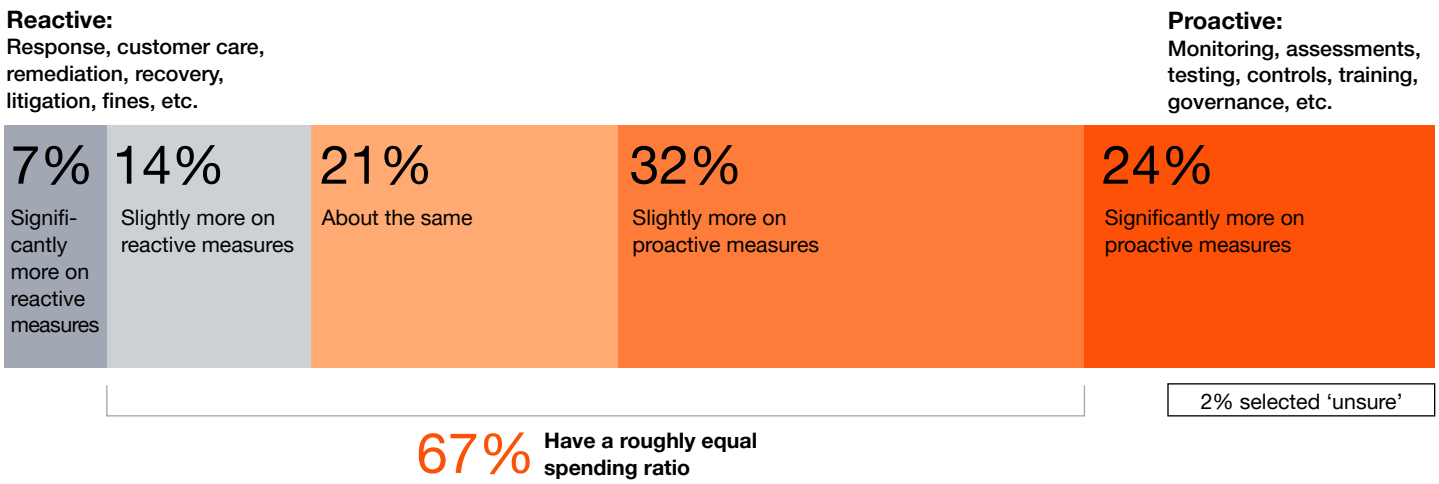
Cybersecurity is about readiness. It means planning ahead and investing in proactive measures like monitoring, assessments, testing, controls and training — **before** a crisis happens. The alternative, relying primarily on reactive measures (e.g., response, customer care, remediation, recovery, litigation and fines), is more costly, risky and unsustainable.

Two-thirds (67%) of organisations say their proactive/reactive cost ratio is roughly even — spending about the same on proactive and reactive cyber measures or slightly more on either. Few (24%) are in the sweet spot of investing significantly more on proactive steps. What's more, those numbers likely underestimate the true cost of reacting. While proactive spending sits in the security leader's budget and is easy to track, reactive costs are dispersed across the business — legal,

communications, operations, IT, product, marketing, government relations — and include harder-to-quantify costs such as lost opportunities and reputational damage.

For that matter, spending on proactive measures won't help if it's focused on the wrong risks or isn't nimble enough to adapt to new conditions. True readiness requires a deep understanding of the risk and threat landscape, one that informs the company's cyber strategy, the people it hires and the processes, systems and tools it adopts.

Spending on reactive vs proactive measures



Q13. Is your organisation spending more resources on reactive or proactive cybersecurity measures? Base: All respondents=3887
Source: PwC 2026 Global Digital Trust Insights

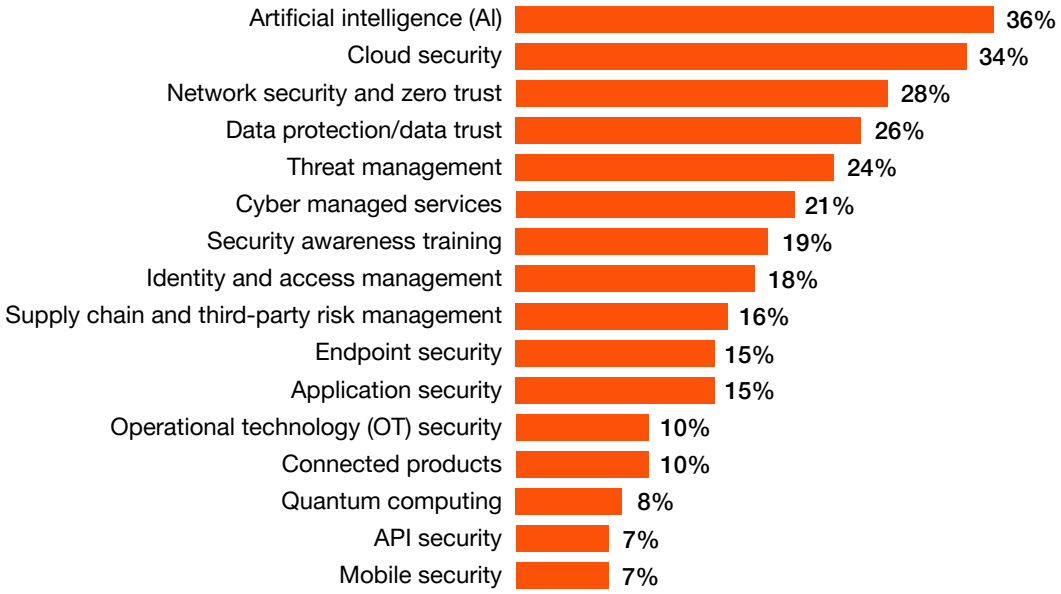
Mapping investment priorities to preparedness

AI and cloud security are the top two cyber budget priorities for the year ahead. That's no surprise. As noted earlier, cloud also tops the list of threats leaders feel least prepared to address. The gap between risk and readiness is being recognised, and funding is following.

But the picture isn't complete. Attacks on connected products rank as the second area where organisations feel least prepared — yet far fewer are allocating budget to it. This mismatch suggests some threats are still flying under the radar.

Cyber managed services are another funding priority for many organisations. High-growth companies are taking this a step further with 30% ranking them among their top three investment priorities. This reflects a strategic move to leverage external expertise and close critical gaps in cyber readiness.

Investments organisations are prioritising when allocating cyber budgets
(% that ranked in their top 3 priorities)

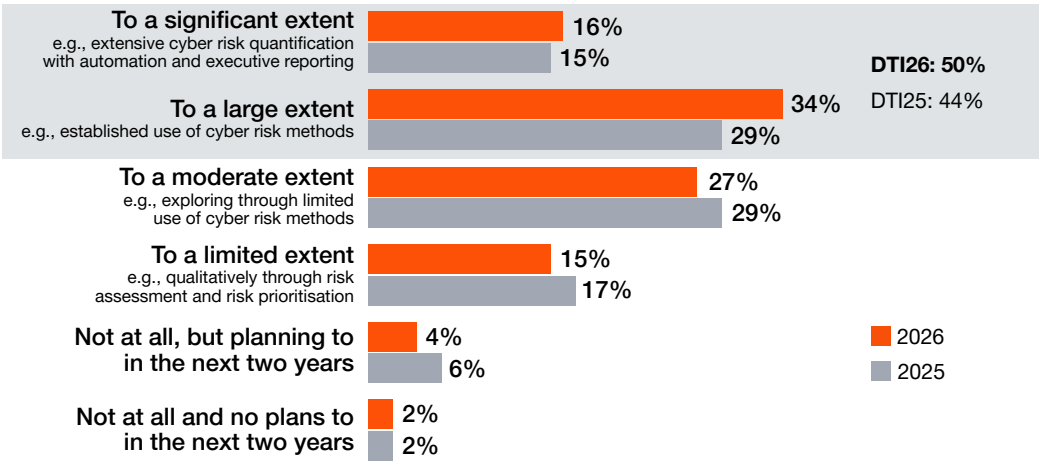


Q9. Which of the following investments are you prioritising when allocating your organisation's cyber budget in the next 12 months? Base: Security leaders=1740
Source: PwC 2026 Global Digital Trust Insights

Putting a price on cyber risk

More organisations are putting numbers behind their risk. Half now report using cyber risk quantification to measure financial impact to a significant or large extent — up from 44% last year. But dig deeper and only 16% are doing this to a significant extent. Business leaders need credible, actionable **cyber risk reporting insights** to assess the threats the organisation faces and judge how best to respond.

Measurement of financial impact of cyber risks



Q12. To what extent is your organisation currently measuring the potential financial impact of cyber risks (i.e., risk quantification)? Base: Security leaders, CFOs, CEOs, CROs and the Board =2673, DTI25: Security leaders, CFOs, CEOs, CROs and the Board=2570
Source: PwC 2026 Global Digital Trust Insights

03

AI in cybersecurity

From promise to priority

#1

cyber investment priority for security leaders is AI

#1

AI security capability prioritised by security leaders is threat hunting

Top 3

areas of priority for agentic AI are cloud security, data protection and cyber defence

AI's potential for transforming cyber capabilities is clear and far-reaching. That's why it ranks highest in several categories we surveyed. AI enablement of key cyber capabilities is the top priority for allocating cyber budgets, using managed cybersecurity services and addressing cyber talent gaps.

To bolster their AI-enabled security capabilities over the next 12 months, security leaders rank threat hunting as their top priority. They're also pursuing other capabilities such as agentic solutions, event detection and behavioural analytics, identity and access management, and vulnerability scanning and assessments.

Agentic AI among the top prioritised AI security capabilities
(Ordered based on those who ranked as their top priority)

Q18. Which of the following AI security capabilities will your organisation prioritise over the next 12 months? Base: Security leaders=1740
Source: PwC 2026 Global Digital Trust Insights

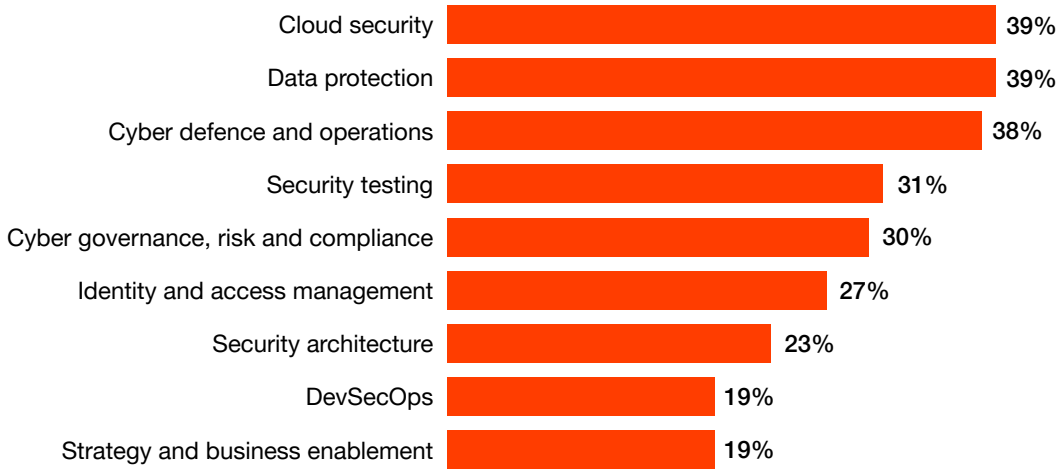
Agents of change in cyber defence

Businesses are recognising that **AI agents** — autonomous, goal-directed systems capable of executing tasks with limited human intervention — have enormous potential to transform their cyber programmes. No longer just tools that provide analysis, these AI systems are evolving into digital assistants that can act independently, collaborate with human teams and even initiate security responses, driving both efficiency and productivity.

That's why security leaders rank AI agents among the top AI security capabilities their organisations are prioritising over the next 12 months.

Where are they planning to deploy these agentic solutions? Cloud security, data protection and cyber defence and operations rank as the top security priority areas for AI agents in the coming year. Other priority areas include security testing, cyber governance, risk and compliance (GRC), and identity and access management.

Agentic AI priorities to increase efficiency and productivity
(% that ranked in their top 3 priorities)



Q19. In which of the following areas will your organisation prioritise agentic AI to increase efficiency and productivity over the next 12 months? Base: Security leaders=1740
Source: PwC 2026 Global Digital Trust Insights

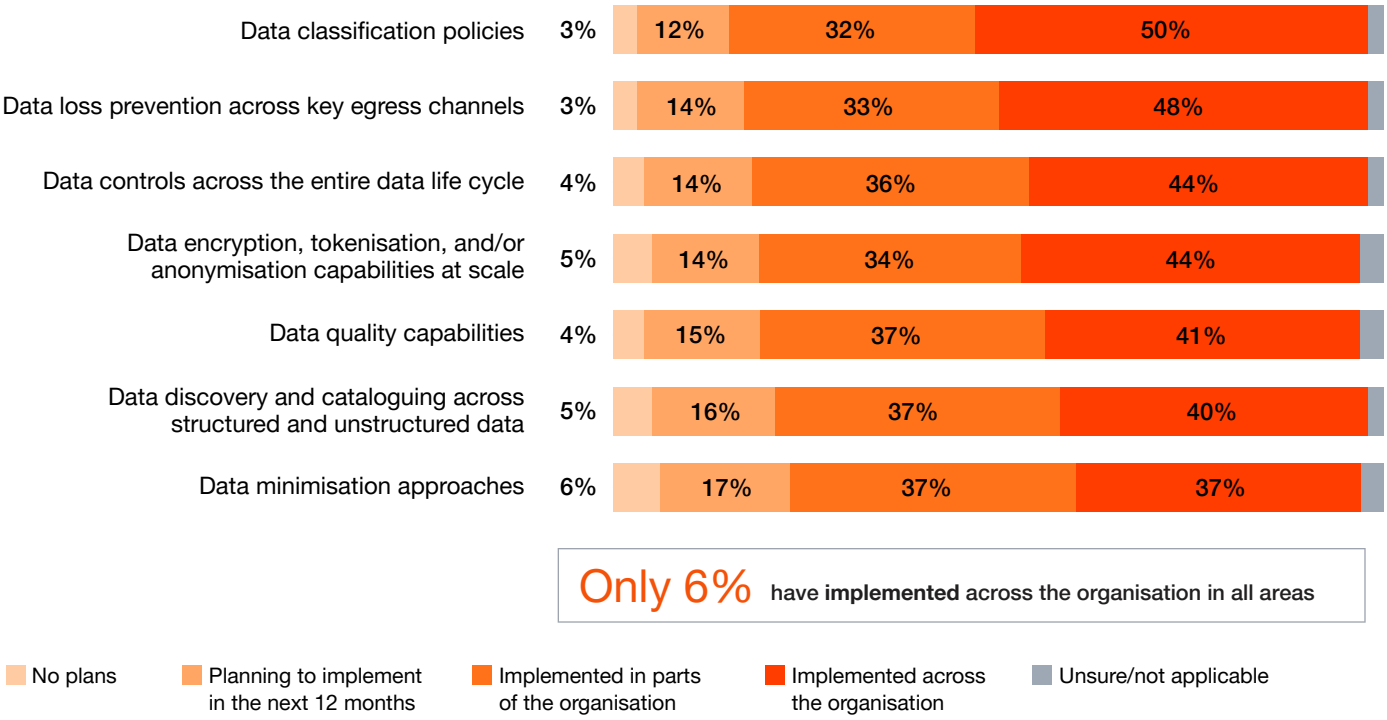
Managing AI data risk

Successful AI deployment and use can't happen without robust **data risk** management practices. That's because effective AI solutions rely on access to curated, high-quality data sets, as well as strong, enterprise-wide governance and security to confirm those data sets are used in the right context.

Are organisations up to the challenge? Asked about their progress implementing various data risk measures across the business, only about half have fully implemented data classification policies (50%) and data loss prevention across key egress channels (48%), while other measures ranked even lower. What's more, only 6% have implemented all measures surveyed across the enterprise.

This gap in readiness shows the work that lies ahead for organisations to unlock the potential of their data for use in AI solutions. Building strong **digital trust** through transparent, responsible and secure data practices will be key to capturing AI-driven innovation and growth.

Implementation of measures to address data risk



Q5. To what extent has your organisation implemented or is planning to implement any of the following measures to address data risk across the enterprise?
Base: Security leaders, CFOs, Finance Directors, CDOs, Chief Counsel/GC/CLO, CROs, Risk Directors, CAEs and Internal Audit Directors=2395
Source: PwC 2026 Global Digital Trust Insights

04

Quantum computing readiness

Preparing for next-level threats

Top 4

threats organisations are least prepared to address now include quantum computing

49%

of organisations haven't considered or started implementing any quantum-resistant security measures

Only 8%

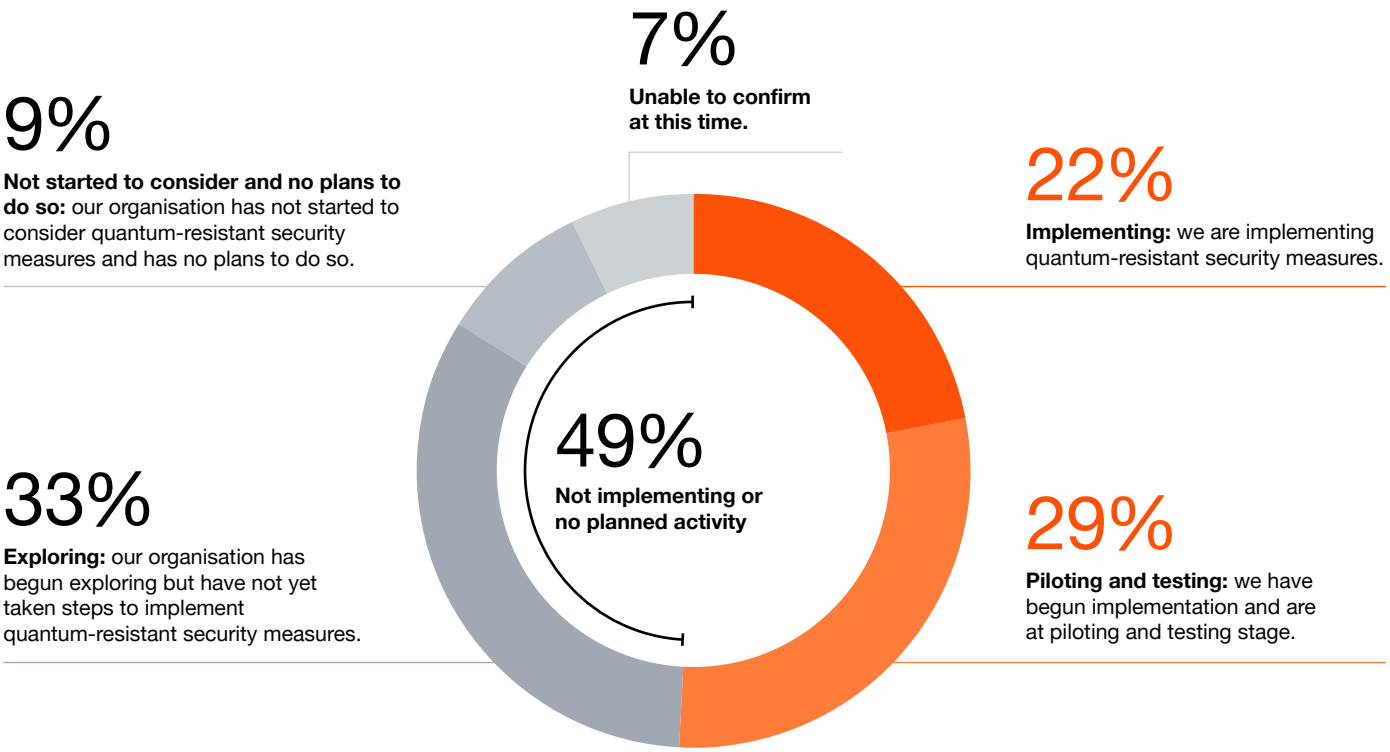
of security leaders include quantum readiness in their top three budget priorities

The quantum computing countdown has begun. No longer theoretical, it's moving beyond the lab and is already introducing new ways to help solve complex problems, such as financial modelling and logistics optimisation, while reshaping decades-long assumptions in cybersecurity.

Although quantum isn't an immediate cyber threat, those who delay the transition to **post-quantum cryptography** may be exposing their sensitive data, authentication services and cryptographic systems. With implementation timelines stretching into years, establishing the foundations for quantum-resistant security demands early action today to avoid adversarial disruption tomorrow.

Some organisations are making initial progress, with 29% in piloting and testing stages. However, only 22% have moved beyond piloting, and almost half (49%) haven't considered or started implementing any quantum-resistant security measures. What's holding them back? For many, it's a lack of understanding around post-quantum risks, combined with limited internal resources and competing demands.

Quantum-resistant security progress



Q21: How far along is your organisation when it comes to quantum-resistant security measures? Base: All respondents=3887
Source: PwC 2026 Global Digital Trust Insights

Quantum concerns grow, but readiness lags

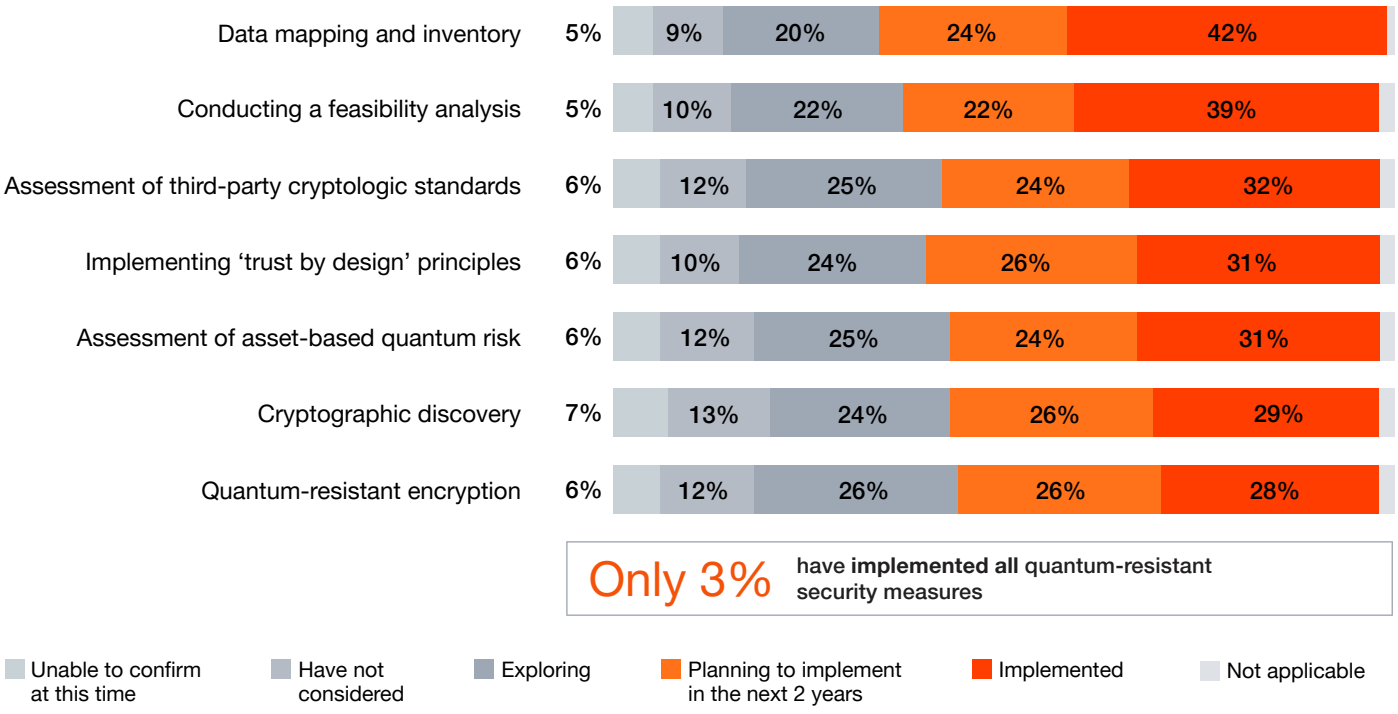
Awareness of quantum threats is growing. Quantum computing now ranks among the top four threats that organisations feel least prepared to address, up several notches from last year.

But are these concerns translating into action? While roughly one-third have implemented one or more quantum-resistant security measures surveyed, only 3% have implemented all seven measures surveyed. Although these steps aren't exhaustive, they're core practices in a multi-year journey that need immediate attention. Looking ahead, only 8% of security leaders include quantum readiness in their top three budget priorities for the coming year.

Organisations with over $5 billion in revenue are more likely to have implemented these steps, including a data inventory to mitigate 'harvest now, decrypt later' risk, cryptographic discovery to identify vulnerable cryptographic assets, testing and implementing quantum-resistant encryption, and conducting feasibility analyses and quantum risk assessments. Higher-growth companies, too, are recognising the cyber challenge quantum presents and are positioning themselves accordingly.

But they remain the exception. As the technology advances, the ability to quickly adopt quantum-resistant cryptography is poised to become a defining enterprise capability.

Implementation of quantum-resistant security measures



Q22. How far along is your organisation when it comes to the following quantum-resistant security measures? Base: Security leaders=1740
Source: PwC 2026 Global Digital Trust Insights

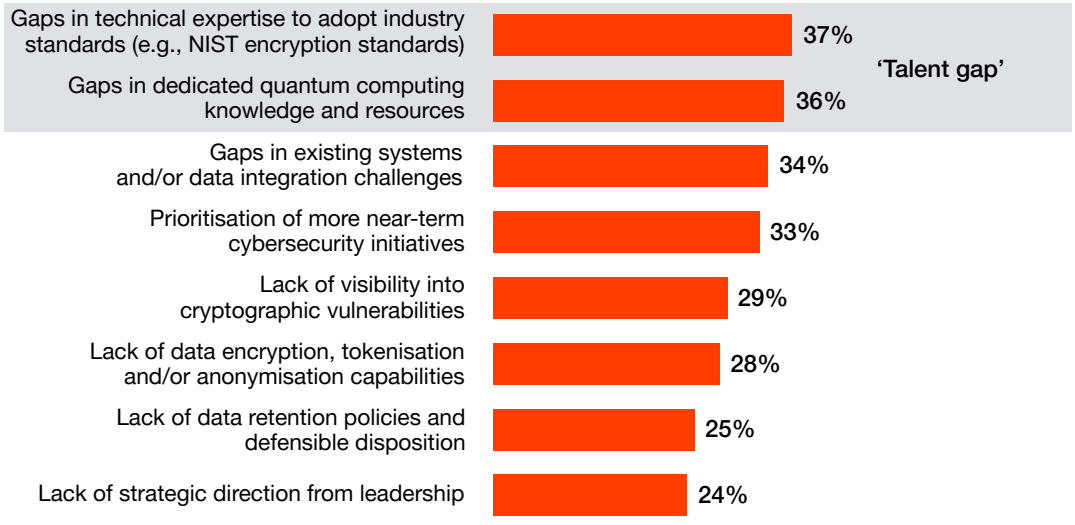
Why post-quantum cryptography is hard

Quantum readiness isn't just a technical upgrade, it's a foundational and strategic shift to future-ready security practices. The top internal barriers? Gaps in technical expertise, limited institutional knowledge and rigid legacy systems.

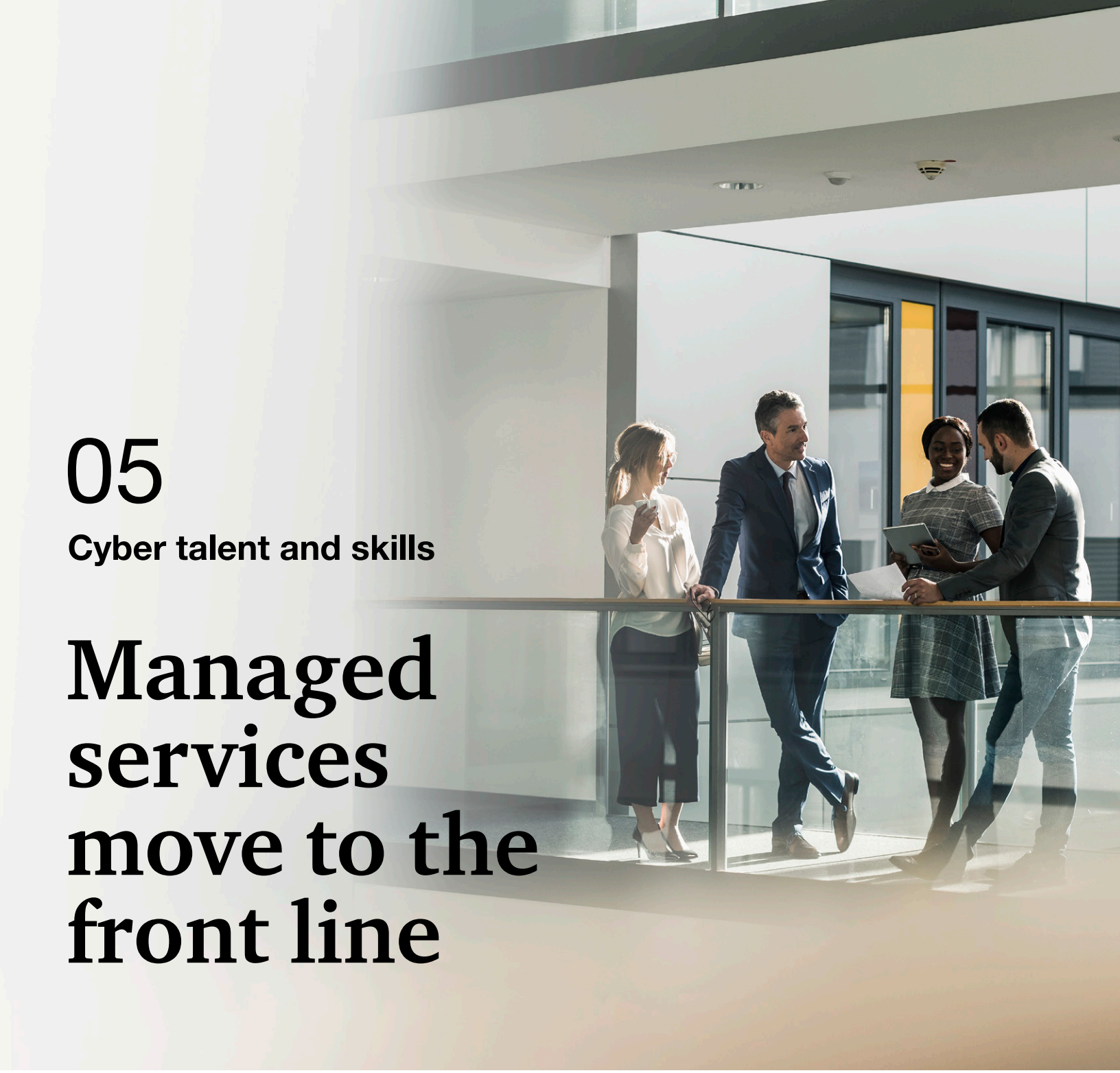
As organisations establish cryptographic inventories to start transitioning to quantum-resistant cryptography, they should identify vulnerable algorithms across their technology stack. While it's widely understood that public key encryption is vulnerable given 'harvest now, decrypt later', security leaders should be aware of technologies they're relying on for authentication and digital signatures using equally vulnerable cryptographic algorithms.

These hurdles make one thing clear: Even when prioritised, starting a cryptographic inventory and implementing quantum-resistant cryptography takes time. And time is in short supply. Leading industry encryption standards — such as those from the US National Institute of Standards and Technology (NIST) — recommend deprecating vulnerable algorithms before threat actors gain quantum computing capabilities. That's why it's critical for companies to close knowledge gaps, assess their cryptographic dependencies and build a roadmap for readiness.

Challenges to achieving post-quantum cryptography
(% that ranked in their top 3 challenges)



Q23. What are your organisation's biggest internal challenges to achieving post-quantum cryptography over the next 12 months? Base: Security leaders=1740
Source: PwC 2026 Global Digital Trust Insights



05

Cyber talent and skills

Managed services move to the front line

Top 2

challenges to implementing AI for cyber defence are knowledge and skills gaps

53%

rank AI and machine learning tools in their top three priorities to address cyber talent gaps over the next 12 months

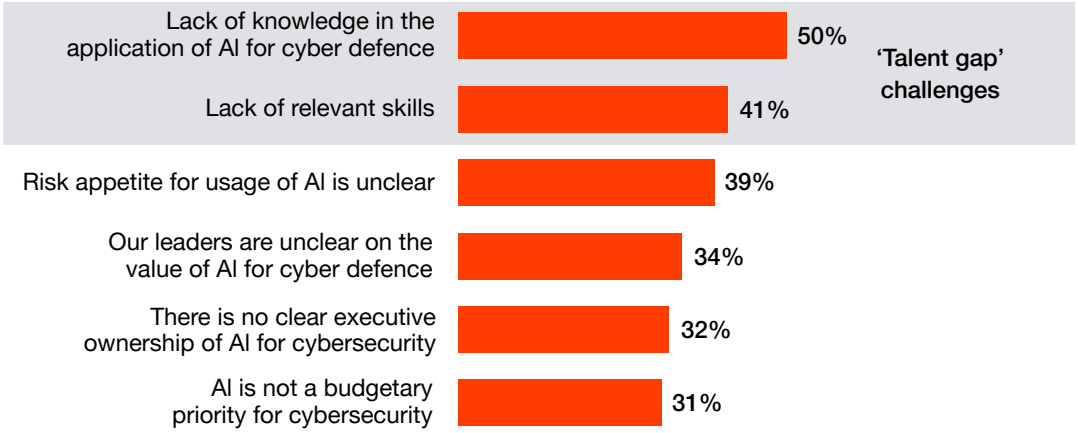
48%

of organisations that have experienced a major attack are prioritising managed services to address cyber talent gaps

Cybersecurity workforce shortages continue to impede progress, especially as organisations push to operationalise AI, secure complex environments and prepare for next-generation threats.

Knowledge and skills gaps were the top two barriers to implementing AI for cyber defence over the past year, forcing organisations to rethink how they scale capabilities. Many are exploring new ways to gain proficiency, including AI tools (53%), security automation tools (48%), cyber tool consolidation (47%) and upskilling or reskilling (47%). They're also prioritising specialised managed services, especially those organisations that have experienced a major attack (48%).

AI implementation challenges for cyber defence
(% that ranked in their top 3 challenges)

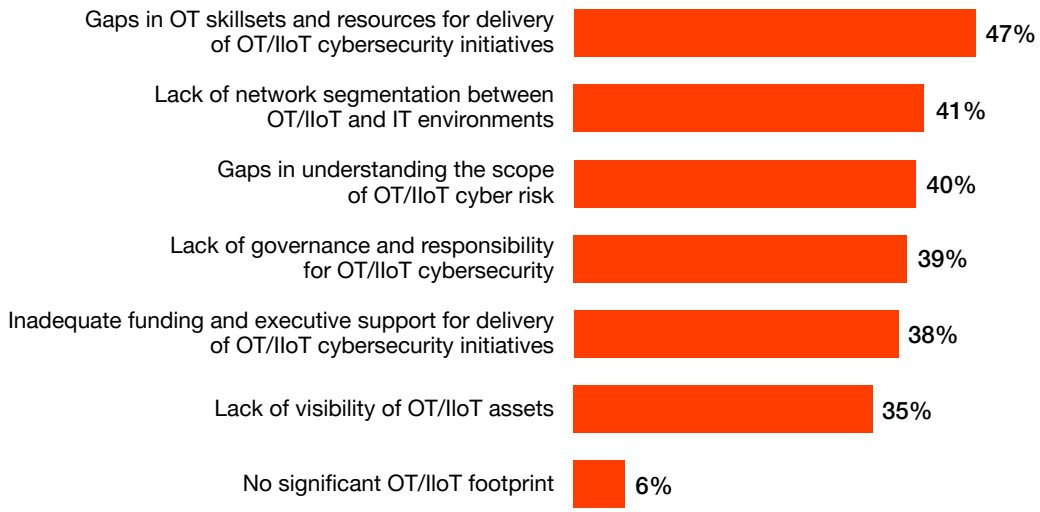


Q20. What have been your organisation's biggest internal challenges to implementing AI for cyber defence over the last 12 months? Base: Security leaders, CEOs, CFOs, Finance Directors, COOs and Operations Directors=2764
Source: PwC 2026 Global Digital Trust Insights

Wanted: Operational technology skills

Operational technology (OT) and industrial internet of things (IIoT) have become pressure points in today's security landscape. Nearly half (47%) of leaders cite a lack of qualified personnel among their top three challenges, while 39% point to unclear governance and ownership. Together, these discrepancies expose a deeper issue, that many organisations still lack the structure and expertise to manage increasingly connected operational systems with confidence.

Obstacles for securing OT and IIoT systems
(% that ranked in their top 3 obstacles)



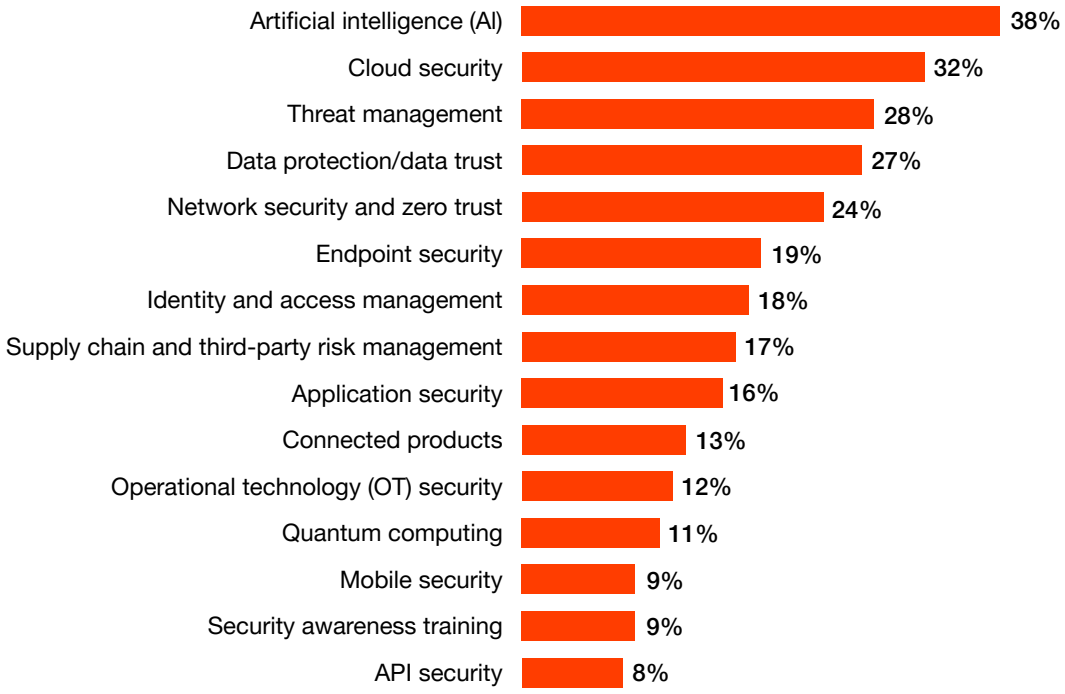
Q4. What are the top 3 challenges your organisation faces in securing operational technology (OT) and/or industrial internet of things (IIoT) systems? Base: Security leaders=1740
Source: PwC 2026 Global Digital Trust Insights

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 get delivered.

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

Cybersecurity priorities for the use of managed services
(% that ranked in their top 3 priorities)



Q15. Which, if any, of the following areas of your cybersecurity programs is your organisation prioritising to utilise managed services over the next 12 months? Base: Security leaders=1740
Source: PwC 2026 Global Digital Trust Insights

C-suite playbook

From uncertainty to action

What leaders can do now

This year's survey shows that the most forward-looking organisations are aligning cybersecurity with business strategy and prioritising readiness over reactivity.

Many have already established foundational cyber risk management practices by reinforcing a governance structure that aligns to leading cyber frameworks, embedding cyber risk controls across the enterprise and prioritising risk assessments and reporting.

To be future-ready, however, you'll need to do more than business as usual. That means confronting uncertainty, making bold but informed decisions and building agility into your strategy.

CISO/CSO

Your ability to not only translate complex cyber risks into business risks but also effectively communicate how cybersecurity is a shared responsibility are key to securing C-suite buy-in and collaboration. This shared understanding will help foster foundational governance, resilience, regulatory compliance and response practices. Moving forward, you should proactively address novel risks by advancing a secure-by-design mindset and use data to measure and show where cyber investments are needed most.

Foundational
Quantify geopolitical risk exposure using metrics tied to critical infrastructure, global operations and industry-specific disruptions and share findings with the C-suite.
Implement dynamic threat modelling aligned to current intelligence on high-risk regions, cyber threat campaigns and data extortion trends.
Embed **Responsible AI** principles across AI deployments and classify AI systems (including models, agents and their identities, applications and training data) based on sensitivity, criticality and exposure.
Secure AI by expanding existing security controls to AI systems and identifying gaps where new capabilities are required (e.g., AI guardrails or LLM gateways).
Regularly reexamine and update cyber risk governance models to incorporate evolving technology risks like AI and quantum.
Strengthen governance through actionable KPIs that track performance in managing third-party, supply chain, legacy and cloud-based risks.
Run tabletop exercises and simulations to stress-test decision-making, determine escalation paths and validate recovery steps.

Future-ready
Establish cybersecurity as a shared responsibility with the C-suite and board by incorporating governance discussions on top of threat intelligence insights and executive-level summaries of emerging threats and adversary capabilities.
Operationalise AI agent oversight and governance through discovery, classification, exposure mapping and continuous monitoring, including adversarial simulations.
Shift from point-in-time vendor assessments to continuous third-party risk monitoring.
Assess which systems depend on cryptography and adopt post-quantum cryptographic (PQC) standards where needed.
Determine if your business should leverage managed services by developing an ROI-based managed services plan that maps technology, skills and resource needs.
Assess your data and determine what should be quantum-ready now, then work with your data governance teams on quantum adoption.

CTO/CIO

Your foundational focus on **securely scaling technology** and proactively addressing talent and training gaps provides critical support to the organisation's cyber posture. You should continue collaborating closely with security leadership to embed risk controls and governance throughout technology adoption. Looking forward, you'll lead efforts to pilot and integrate emerging technologies like AI and quantum computing with built-in security while driving innovation that anticipates and mitigates future cyber risks.

Foundational
Scale AI and other emerging technologies securely, budgeting for and embedding critical proactive security measures.
Collaborate closely with CISO and CRO to align technology deployment with risk management and compliance requirements.
Secure AI by embedding governance and cyber risk controls in AI implementation planning from the start, aligned with secure-by-design principles.
Enforce consistent identity, access and policy controls across third-party platforms, APIs and integrations.
Apply robust IIoT and OT governance into your architecture strategy to gain end-to-end visibility and controls across distributed environments.

Future-ready
Coordinate with CISOs and data leaders to secure sensitive training data and reinforce AI model input/output governance.
Align quantum adoption and pilot initiatives with enterprise-wide quantum-resistant security strategies in partnership with security leadership.
Advance adoption of automation and AI-driven risk detection and response tools to increase operational efficiency and resilience.
Adopt a secure-by-design framework for connected products throughout the operational life cycle.

CRO

Your focus on identifying enterprise and emerging risks, and their interdependencies with cybersecurity, is critical to safeguard the organisation. You should continue tailoring controls for evolving vulnerabilities while confirming that risk frameworks are still current. Looking ahead, your role will continue to require integrating AI, quantum and geopolitical exposures into an adaptive, forward-looking risk management strategy that supports the organisation's agility and resilience.

Foundational
Embed threat-led scenarios into risk registers and stress testing cycles, prioritising threats with known geopolitical vectors.
Evaluate existing controls to address these exposures, tailoring current mitigation strategies where necessary.
Quantify AI and quantum risks using tailored business impact analyses, prioritising areas with **digital workforce automation**.
Support compliance efforts by mapping cyber threat management to regulatory requirements.

Future-ready
Expand third-party risk models to consider quantum capability in vendor environments and resilience to adversarial AI misuse.
Leverage AI to continuously assess cyber risk at scale, from cyber risk quantification through assessments to reporting.
Develop an intelligence-integrated risk framework (IIRF) that incorporates various lenses of strategic threat intelligence into enterprise risk scoring.
Pilot predictive threat modelling tools to simulate emerging threats and quantify probable business impacts over the next 12 to 36 months.

CFO

Your foundational role in enforcing appropriate budgeting for proactive cyber measures in strategic initiatives and tech implementations is essential to organisational resilience. You should continue identifying inefficiencies and aligning budgets with high-impact cyber initiatives. Looking ahead, preparing for emerging risks means proactively mapping future budget needs and fostering **ROI-driven funding models** so the organisation can invest wisely in security technologies and skills.

Foundational
Support strategic investments that drive long-term resilience, competitive advantage and regulatory readiness.
Assess the long-term costs of reacting to security incidents versus investing proactively in cyber defences, managed services, insurance, compliance, etc.
Recalibrate cyber ROI metrics to include savings from incident prevention, regulatory fines avoided and response time reduction.
Collaborate with CISOs, CTOs and CIOs to budget effectively for cybersecurity skill development and technology training.
Support sustainable funding models that balance operational costs with strategic cyber investments.

Future-ready
Advocate for cybersecurity as a material business function, linking investment levels to board-level performance objectives.
Create a capital allocation reserve for ‘resilience enablers’, including zero-day exploitation response capabilities and post-quantum hardening.
Develop ROI-driven business cases for managed security services.
Identify and reduce inefficiencies such as tool redundancies and consolidate where possible.

CEO

Your ongoing commitment to making sure cybersecurity is a business priority remains essential. You should continue aligning business initiatives with the cyber risk management strategy while fostering collaboration across the board and C-suite. Looking ahead, your role involves building influential partnerships and championing investments that enable your organisation to navigate emerging cyber challenges.

Foundational
Mandate cyber scenario participation at executive offsites, simulating sector-specific disruptions and hybrid threat operations.
Tie cyber resilience to revenue enablement, such as securing digital platforms, customer data trust and cross-border growth.
Advocate responsible innovation, confirming that AI and quantum projects embed ethical and security guardrails from inception.
Understand where cyber budget trade-offs are made and if those trade-offs meet risk appetite.
Make cybersecurity a shared responsibility at every level, from the boardroom to the back office.
Keep the board informed on strategic cyber programme priorities and engage directors to discuss programme needs.

Future-ready
Lead multi-industry alliances for post-quantum standardization, joint defense postures and threat intelligence exchange.
Champion investment in emerging technologies (AI, quantum) with security designed from the start.
Institutionalise quantum and geopolitical foresight reviews into strategic planning cycles and board risk charters.
Actively participate in stress tests to prepare for geopolitical and technological disruptions.

About this report

The 2026 Global Digital Trust Insights survey has been designed to capture the views of 3,887 business and technology executives conducted in the May through July 2025 period.

One-third of the executives (33%) are from large companies with $5 billion or more in revenue. Respondents operate in a range of industries, including financial services (21%); industrial manufacturing and automotive (21%); tech, media and telecom (19%); retail and consumer markets (16%); healthcare (10%); energy, utilities and resources (9%); and government and public services (4%).

Respondents are based in 72 countries. The regional breakdown of responses is Western Europe (32%), North America (27%), Asia Pacific (18%), Latin America (11%), Central and Eastern Europe (6%), Africa (4%) and the Middle East (3%).

The Global Digital Trust Insights survey had been known as the Global State of Information Security Survey (GSISS). Now in its 28th year, it's the longest-running annual survey on cybersecurity trends. It's also the largest survey in the cybersecurity industry and the only one that draws participation from senior business executives, not just security and technology executives.

PwC Research, PwC's global Centre of Excellence for market research and insight, conducted this survey.

Contact us

Sean Joyce
Principal, Global Cybersecurity and Privacy Leader
PwC United States
sean.joyce@pwc.com | **LinkedIn**