

pwc

Moving targets: Cybersecurity in a dynamic digital world

Findings from the 2027 Global Digital Trust Insights

October 2026

Build resilience for constant change.

No. 1

cyber threat organisations are least prepared to address is attacks targeting AI systems

84%

expect their cyber budget to increase, with AI as a top investment priority

Only

39%

have fully formalised operational continuity plans that specifically address cyber threats

Simultaneous shifts in the technologies organisations rely on, the threats they face, and the geopolitical conditions in which they operate have created a world of moving targets. In this environment, even organisations with strong cyber foundations must rethink what it means to be resilient.

AI is accelerating this change, reshaping both the opportunities organisations pursue and the risks they should manage. Frontier AI models in particular are raising the stakes, testing the assumptions on which security programs were built. The pace of change itself is a core cybersecurity challenge.

Leading through volatility will increasingly distinguish the most successful global businesses. Organisations should strengthen today's cybersecurity foundations while building the agility to adapt to whatever comes next. That takes more than new technologies. It demands resilient operations, trusted data, and the ability to turn intelligence into action across the enterprise.

PwC's 2027 Global Digital Trust Insights survey of 3,934 business and tech leaders across 71 countries reveals how leaders are managing cybersecurity in a rapidly evolving digital environment and where critical gaps remain.

Among the key findings:

- **Security for AI has taken centre stage:** Protecting AI systems has become the most significant cyber preparedness gap. Security leaders identify attacks targeting AI systems as the top cyber threat they're least prepared to address.
- **Cyber spending is back:** After a few years of relatively flat cyber budgets, organisations are doubling down on their investment, with AI being a key driver. Among security and finance leaders, 84% expect budgets to increase—six percentage points higher than last year—and 58% of security leaders rank AI in their top cyber budget priorities.
- **The trust gap in autonomous agents:** Organisations are eager to put AI agents to work for cyber defence, but far less willing to put them in charge. Only 22% would authorise fully autonomous AI actions, with reliability and maturity concerns being the biggest barriers.
- **When the lights go out:** Keeping the business running, even through disruption, is the ultimate goal of cybersecurity. But surprisingly, only 39% of security, risk, and operations leaders have fully formalised and integrated operational continuity plans that specifically address cyber risks, even though cyber incidents have become a matter of when, not if.
- **Strong foundations matter more than ever:** As organisations focus on emerging threats and leveraging data for use in AI systems, many are doing so without fully securing the data they're entrusted to protect. On average, companies have implemented only three out of seven key data risk measures across their organisations.
- **Who's accountable for AI?** No single ownership model has emerged for AI governance and risk management: 29% of CEOs and security and risk leaders say accountability sits with the CIO, CTO, or technology function; 26% with a dedicated AI leader or AI function; and 17% with the CISO or cyber function.
- **Managed services extend critical capabilities:** Organisations are turning to strategic partners for specialised expertise as technologies and threats evolve. AI (53%) and cloud security (49%) rank among their top priorities for managed security services over the coming year.

Navigating a world of moving targets requires a fundamentally different approach. Our C-suite playbook translates this year's findings into practical actions that leaders—CEOs, CISOs, CIOs/CTOs, CDOs, CFOs, and others—can take to build trusted foundations and accelerate the move towards a more **intelligent enterprise**, one that connects the entire organisation to make better decisions and adapt with speed and confidence.

Table of contents



01 Risk and threat landscape
AI vulnerabilities take centre stage 05



02 Cyber strategy and operations
Resilience requires more than investment 11



03 AI for security
Unlocking AI's defensive potential 18



04 Leadership, talent, and governance
A foundation for cyber resilience 23



05 C-suite playbook
What leaders can do to keep pace in a dynamic digital world 31

About this report 40

Contact us 40



01

Risk and threat landscape

AI vulnerabilities take centre stage

No. 1

cyber threat organisations are least prepared to address is attacks targeting AI systems

50%

are changing third-party and supply chain risk management strategies in response to geopolitics

Only

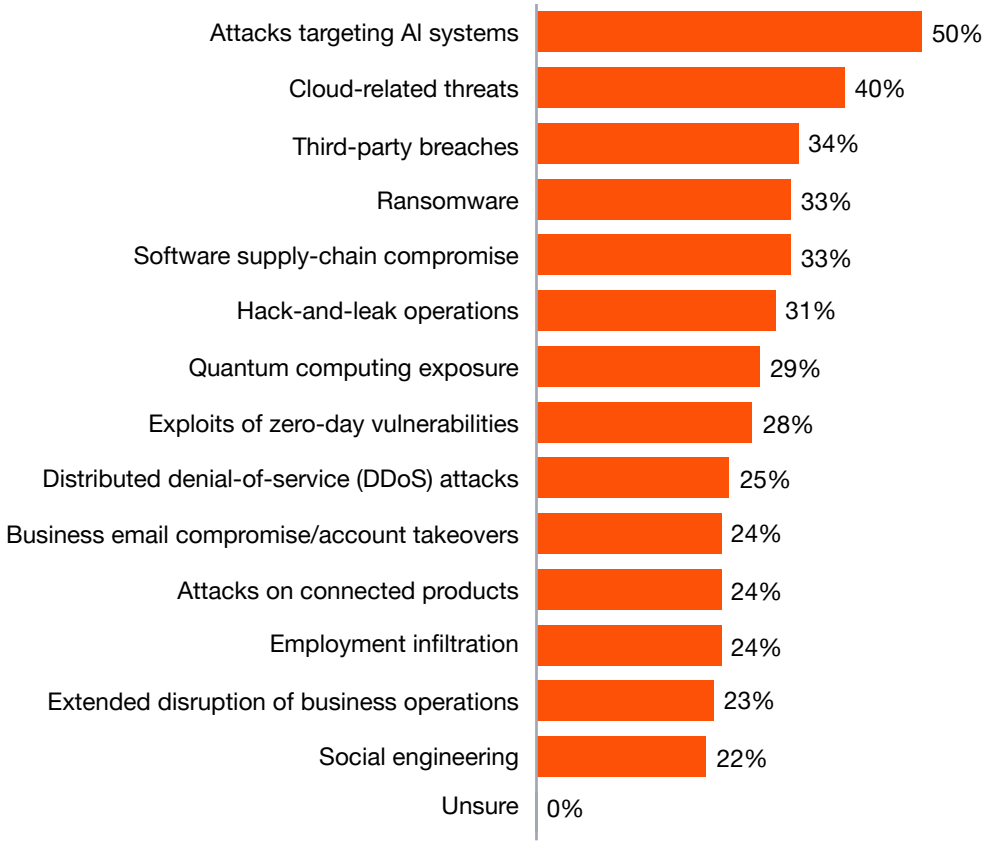
21%

are implementing quantum-resistant security measures

Amid a complex risk and threat landscape, AI has emerged as the biggest challenge. Half (50%) of security leaders identify attacks targeting AI systems as one of their biggest preparedness gaps, followed by cloud-related threats (40%), third-party breaches (34%), and ransomware (33%). Security for AI has emerged as the most acute preparedness gap, underscoring that deployment speed and security cannot be treated as competing choices.

As organisations move quickly to capture AI's value, security, governance, and risk management need to develop alongside it from the outset. This is particularly important as AI-driven operations increasingly rely on external models, platforms, data, and services that can extend third-party exposure.

Cybersecurity threats organisations are least prepared to address in the next 12 months (% that ranked in their top 5 threats)



Q1. Over the next 12 months, which of the following cyber threats is your organisation least prepared to address?
Base: Chief AI officer, CIO, CISO, CSO, CTO, and director/VP/head equivalent respondents (1819)
Source: PwC 2027 Global Digital Trust Insights

Frontier AI changes everything

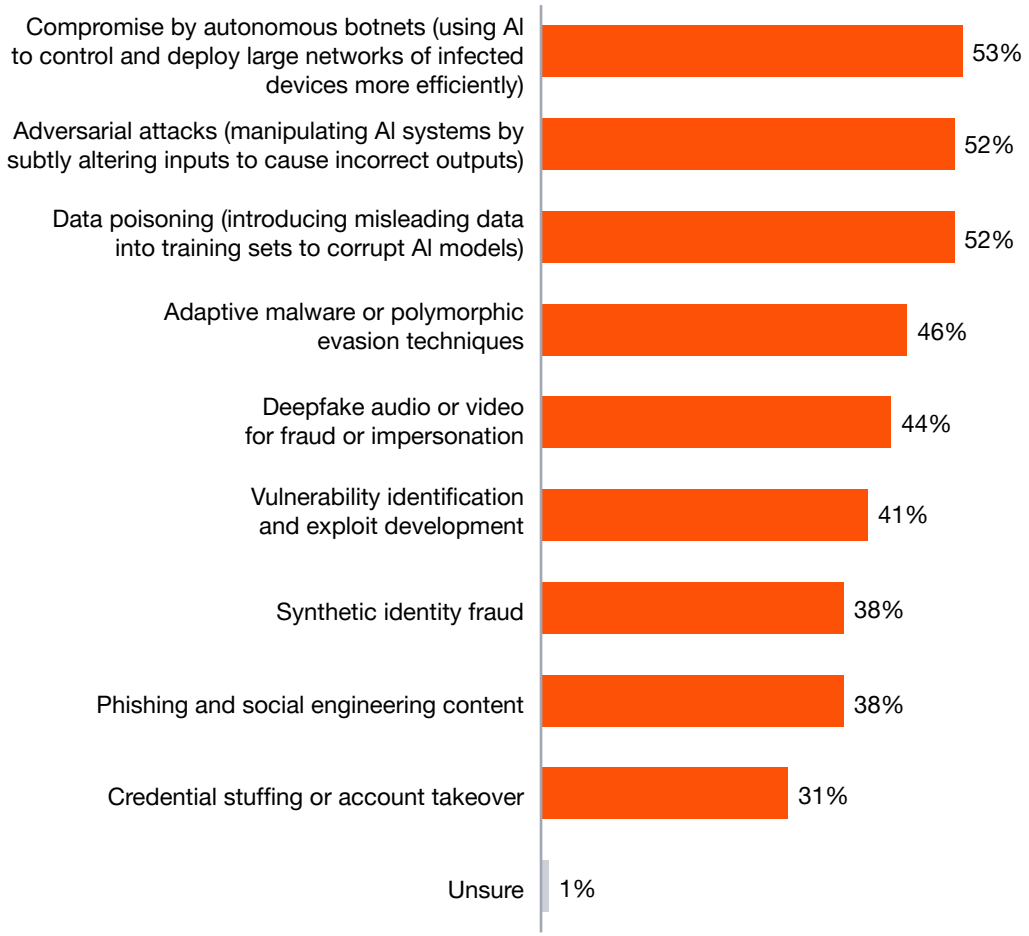
Frontier AI models are now exceptionally good at finding previously unknown software vulnerabilities and exploiting those weaknesses through sophisticated attack paths with minimal human intervention. They're also highly effective at identifying network misconfigurations, unpatched devices, and default credentials.

As frontier AI reshapes the threat landscape, organisations are increasingly concerned about AI-enabled attacks. Security and risk leaders rank compromise by autonomous botnets (53%), adversarial attacks (52%), and data poisoning (52%) as the top AI-enabled attacks they're least prepared to address.

"Artificial intelligence is rapidly changing both the speed and scale of the cyber threat. While AI systems are creating new efficiencies and opportunities for innovation, those same capabilities can be exploited by cybercriminals and nation-state threat actors. To stay ahead of this threat, we must responsibly use AI to strengthen our defense, accelerate disruption, and impose cost on adversaries."

Brett Leatherman
FBI Assistant Director, Cyber Division

AI-enabled attacks organisations are least prepared to address in the next 12 months (% that ranked in their top 5 AI-enabled attacks)



Q2. Over the next 12 months, which of the following AI-enabled attacks is your organisation least prepared to address?
Base: Chief AI officer, CIO, CISO, CSO, CTO, and director/VP/head equivalent, CIRO, CRO, and Risk Director respondents (1976)
Source: PwC 2027 Global Digital Trust Insights

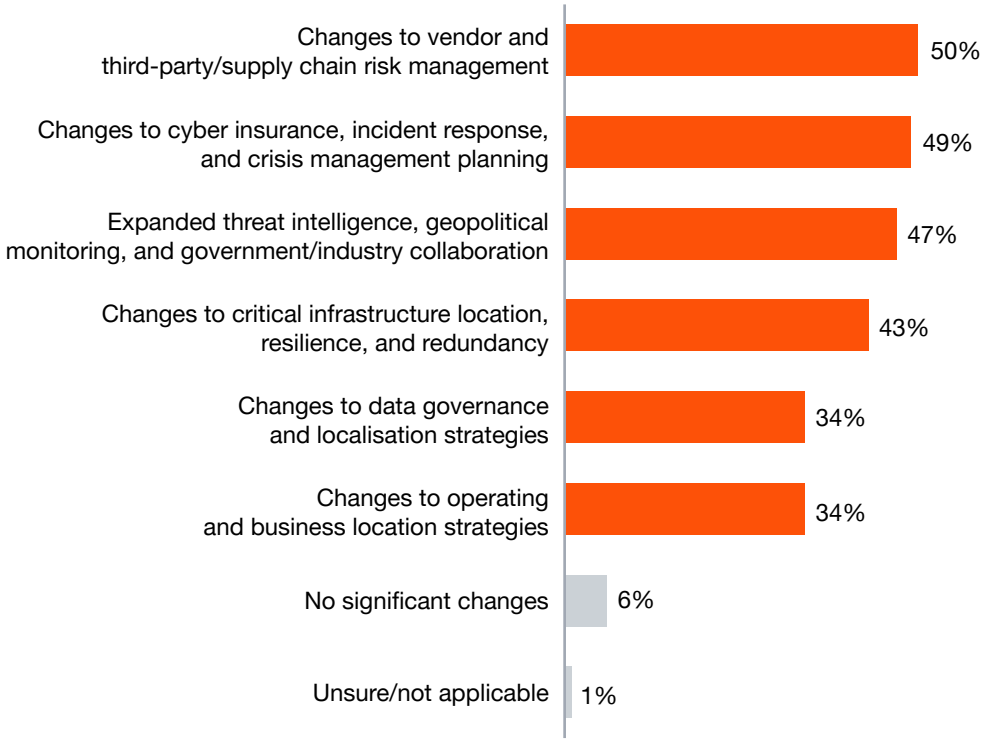
The forces shaping cyber risk are multiplying

Geopolitics is reshaping the cyber risk landscape in new ways. Cyber operations are now a persistent feature of geopolitical competition in both conflict and peacetime. Nation-states continue to use cyber capabilities to advance strategic objectives through persistent presence, theft, and, in limited cases, disruption and destruction. The reach of these operations across digital and physical environments is expanding the scope of cybersecurity, as **operational technology (OT)** and physical infrastructure critical to business is targeted by both kinetic and cyber attacks.

Organisations have been forced to adapt. Half (50%) are making changes to vendor, third-party, and supply chain risk management, while 49% are making changes to cyber insurance, incident response, and crisis management to help bolster their defences against geopolitical threats.

Companies are paying more attention to their software supply chain as they diversify suppliers and strengthen development pipelines. At the same time, frontier AI is democratising software creation—enabling more code, APIs, and cloud configurations to be developed outside traditional engineering teams—and often bypassing established security reviews. This expanding attack surface creates new blind spots, forcing organisations to rethink how they secure their rapidly evolving, interconnected ecosystems amid growing geopolitical uncertainty.

Areas where cyber strategy is changing in the next 12 months in response to the current geopolitical landscape (% that ranked in their top 3 areas)



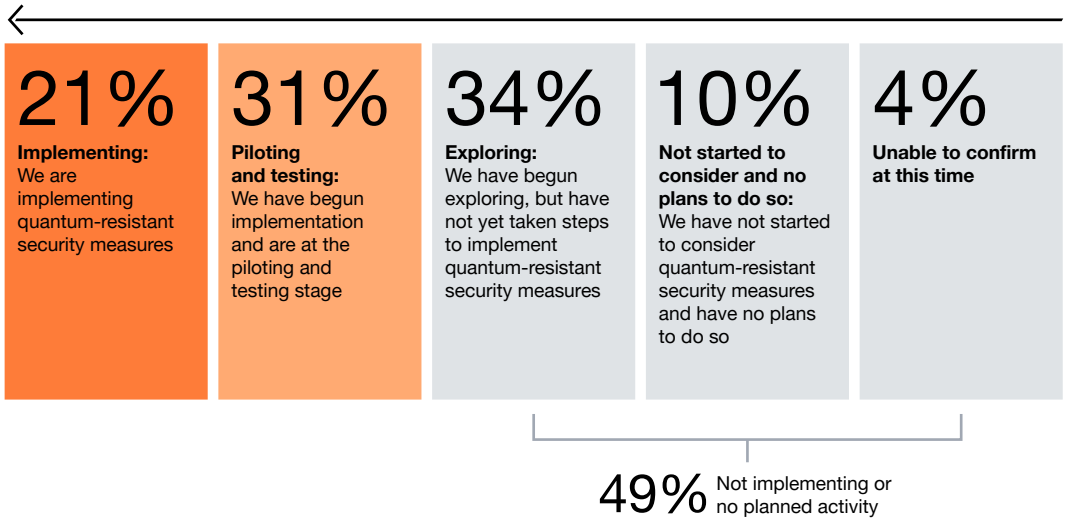
Q3. Which of the following areas in your organisation's cyber strategy, if any, are changing in response to the current geopolitical landscape over the next 12 months?
Base: All respondents (3934)
Source: PwC 2027 Global Digital Trust Insights

Planning for tomorrow's threats?

The next cybersecurity challenge already looms on the horizon. Quantum computing exposure ranks seventh among the threats organisations feel least prepared to address. CISOs, however, place it fourth among their top concerns, suggesting that those closest to cyber risk see a greater urgency to prepare. The **transition to quantum-resistant security** will take years, not months, meaning companies should start preparing now to be ready when **Q-Day** arrives.

Still, only 21% of organisations are implementing quantum security measures, while nearly half (49%) have not even begun. Among those who have at least started to explore quantum-resistant security measures, only about one-third are currently implementing key initiatives like forming a dedicated quantum team and inventorying cryptographic assets. More telling, just 5% are currently implementing security measures across all six quantum readiness initiatives surveyed, highlighting how few are preparing in a holistic way.

Level of maturity in quantum-resistant security measures



Q22a. How far along is your organisation when it comes to quantum-resistant security measures?
Base: All respondents (3934)
Source: PwC 2027 Global Digital Trust Insights



02

Cyber strategy and operations

Resilience requires more than investment

84%

expect their cyber budget to increase in 2027, with 58% ranking AI in their top cyber budget priorities

Only

39%

have a fully formalised, integrated operational continuity plan that addresses cyber risks

Only

5%

have fully implemented all data risk measures surveyed

Cyber spending is back. After a few years of relatively flat investment, 84% of security and finance leaders say they are increasing cybersecurity budgets to respond to these evolving threats, with AI emerging as one of the top areas for investment. That's a six-percentage-point increase from last year. But will this renewed emphasis on investment translate into resilience?

When asked what factors are influencing their cyber spend priorities for the coming year, about half (51%) ranked 'data protection and trust' as their top choice. Close behind were securing against AI-enabled attacks (46%), and securing AI and autonomous agents (45%).

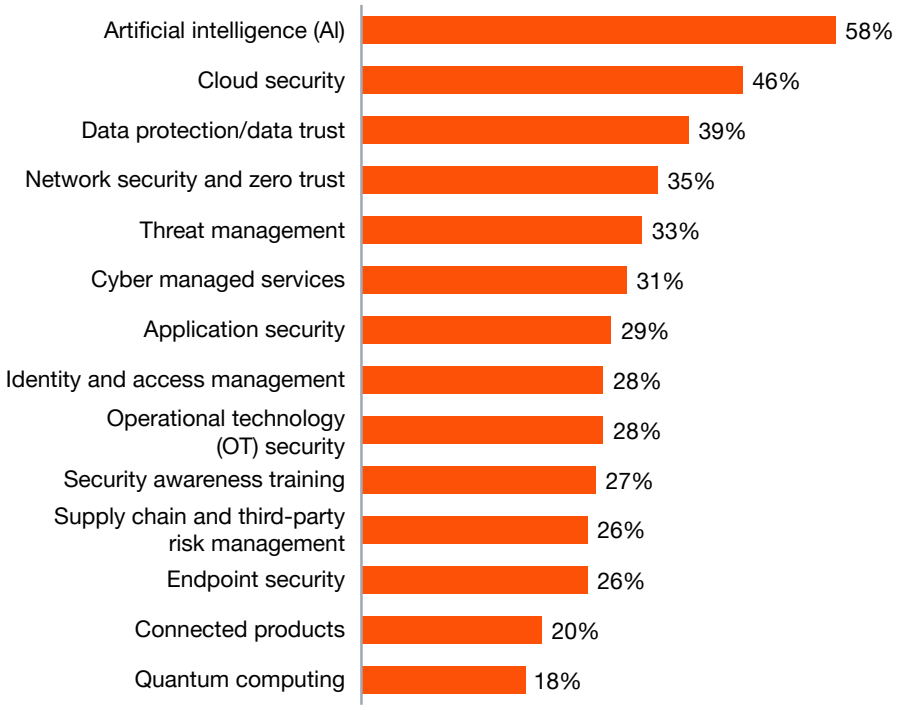
Investments reflect threat priorities

AI and cloud continue to dominate cyber spend priorities, with 58% of security leaders ranking AI among their top five areas for investment. Within those investments, 'responsible AI governance and compliance' tops the list of AI-specific priorities (42%), followed by platform hardening (38%) and supply chain security (35%).

The complex threat environment is moving too fast for many companies to handle alone, so they're bringing in managed services to help protect and defend their enterprise and move from episodic to always-on security. AI and cloud also rank as the top two areas for managed security services as organisations confront a shortage of specialised cyber and AI talent. Experience that spans governance, security, engineering, and ongoing oversight can be augmented through strategic partners.



Investments organisations are prioritising when allocating their cyber budget in the next 12 months (% that ranked in their top 5 investment priorities)



Q9. Which of the following investments are you prioritising when allocating your organisation's cyber budget in the next 12 months?
Base: Chief AI officer, CIO, CISO, CSO, CTO, and director/VP/head equivalent respondents (1819)
Source: PwC 2027 Global Digital Trust Insights

You're only as resilient as your ecosystem

Organisations are planning changes to their enterprise tech stacks to reduce concentration risk. As dependence on cloud providers and third-party technology grows, many are taking steps to avoid single points of failure. More than half (54%) of security and risk leaders are adopting multi-cloud or hybrid cloud strategies, while 47% are strengthening regional data and tech redundancy, and 37% are localising infrastructure within specific jurisdictions, to improve resilience and maintain operations during disruption.

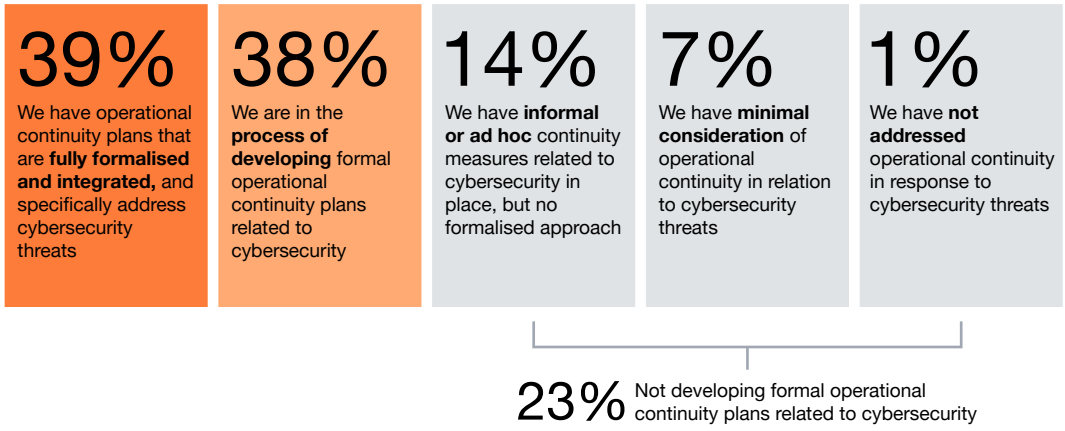
These measures are becoming more important as **geopolitical competition shapes technology sourcing**, provider choice, and where infrastructure and data are located. In making these decisions, organisations should weigh trade-offs across cost, quality and operational sustainability, security and data, and interoperability.

Foundational cybersecurity is lagging behind

Keeping the business running, even through disruption, is the ultimate goal of cybersecurity. After a cyber attack or geopolitical disruption, being able to maintain critical operations, or quickly resume them, is a basic security function. Still, only 39% of security, risk, and operations leaders report that their cyber continuity plans are fully formalised. Another 23% have no formal plans in place.

Formal plans are just the starting point. Operational resilience goes beyond documentation. It requires business continuity, technology recovery, and crisis response to be integrated into the day-to-day operations and regularly tested before they're needed. Defining the **minimum viable company**—the smallest set of capabilities needed to keep the organisation operating through disruption—helps establish what must be maintained or restored first.

Approach to operational continuity planning in response to the current cyber threat landscape



Q15. Which of the following best describes your organisation's approach to operational continuity planning in response to the current cyber threat landscape?
Base: Chief AI officer, CIO, CISO, CSO, CTO, and director/VP/head equivalent, CEO, COO, Operations Directors, CRO and Risk Director respondents (2725)
Source: PwC 2027 Global Digital Trust Insights

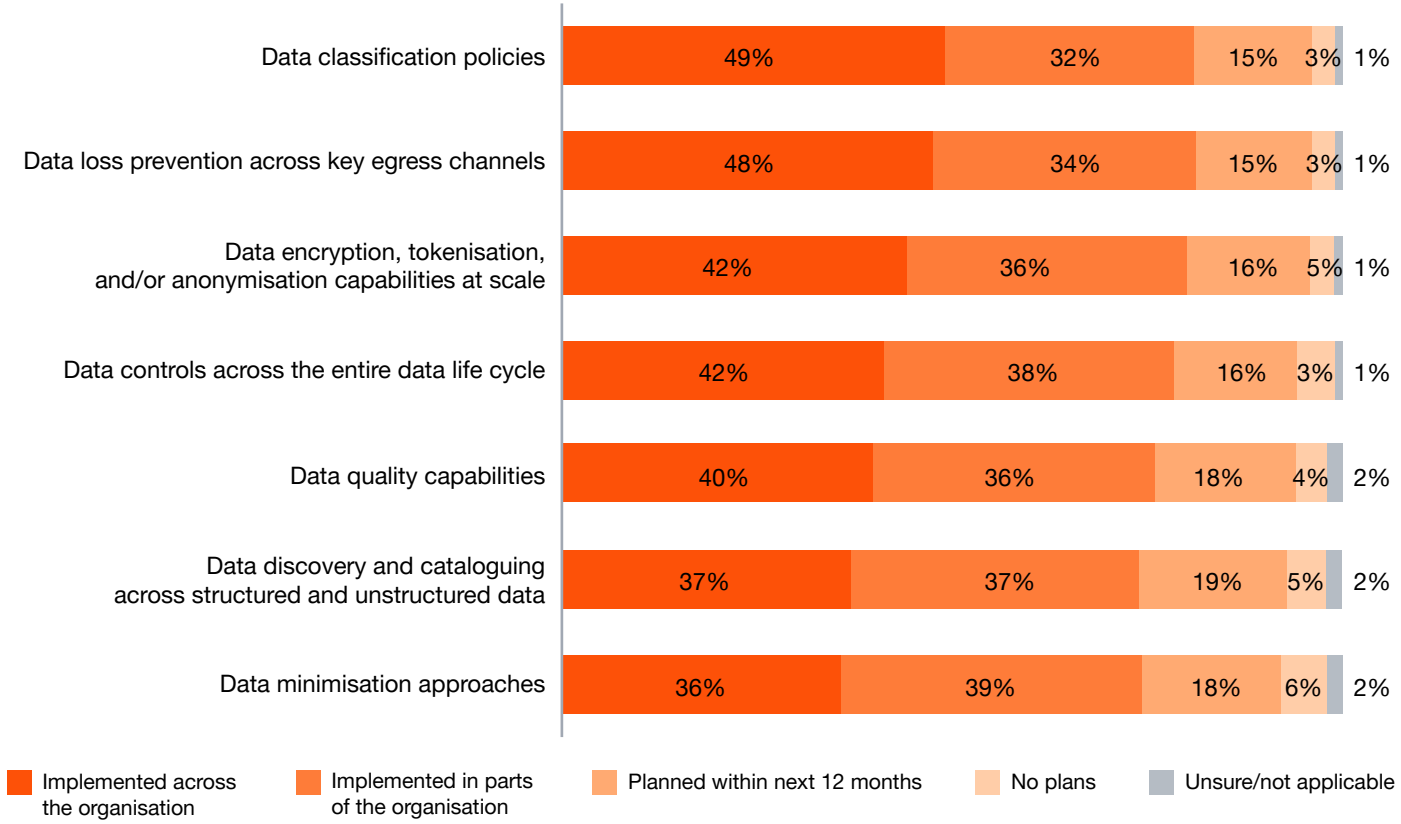
The data foundation gap is widening

AI is only as trustworthy as the data beneath it. Organisations consistently rank data protection and trust as their top cybersecurity investment priority. But many are pursuing AI and other emerging technologies without fully securing one of their most important assets: data. Even in the face of rising frontier AI vulnerabilities, companies have implemented only three out of seven leading data risk measures across their organisations. What's more, only 5% have fully implemented every data risk measure surveyed, down from 7% last year. This key gap identified in last year's survey has not only persisted but widened.

Beyond this, the fundamentals of data protection still need work. Only about half of organisations have fully implemented data classification policies (49%) and data loss prevention across key egress channels (48%), while other measures ranked even lower. These foundational capabilities become even more critical when AI, cloud, and connected ecosystems come into play. Organisations can't build cyber resilience on an insecure data foundation.



Measures to address data risk



Q6. To what extent has your organisation implemented any of the following measures to address data risk across the enterprise?
Base: Chief AI officer, CIO, CISO, CSO, CTO, and director/VP/head equivalent, CFO, Finance Director, CDO, Chief Counsel, CIRO, CRO, Risk Director, CAE, Internal Audit Director, Chief Compliance Officer, and Compliance Director respondents (2594)
Source: PwC 2027 Global Digital Trust Insights

"AI is creating both a new class of security risk and one of the biggest opportunities defenders have had in decades. The challenge is building trust and control at the same speed as adoption."

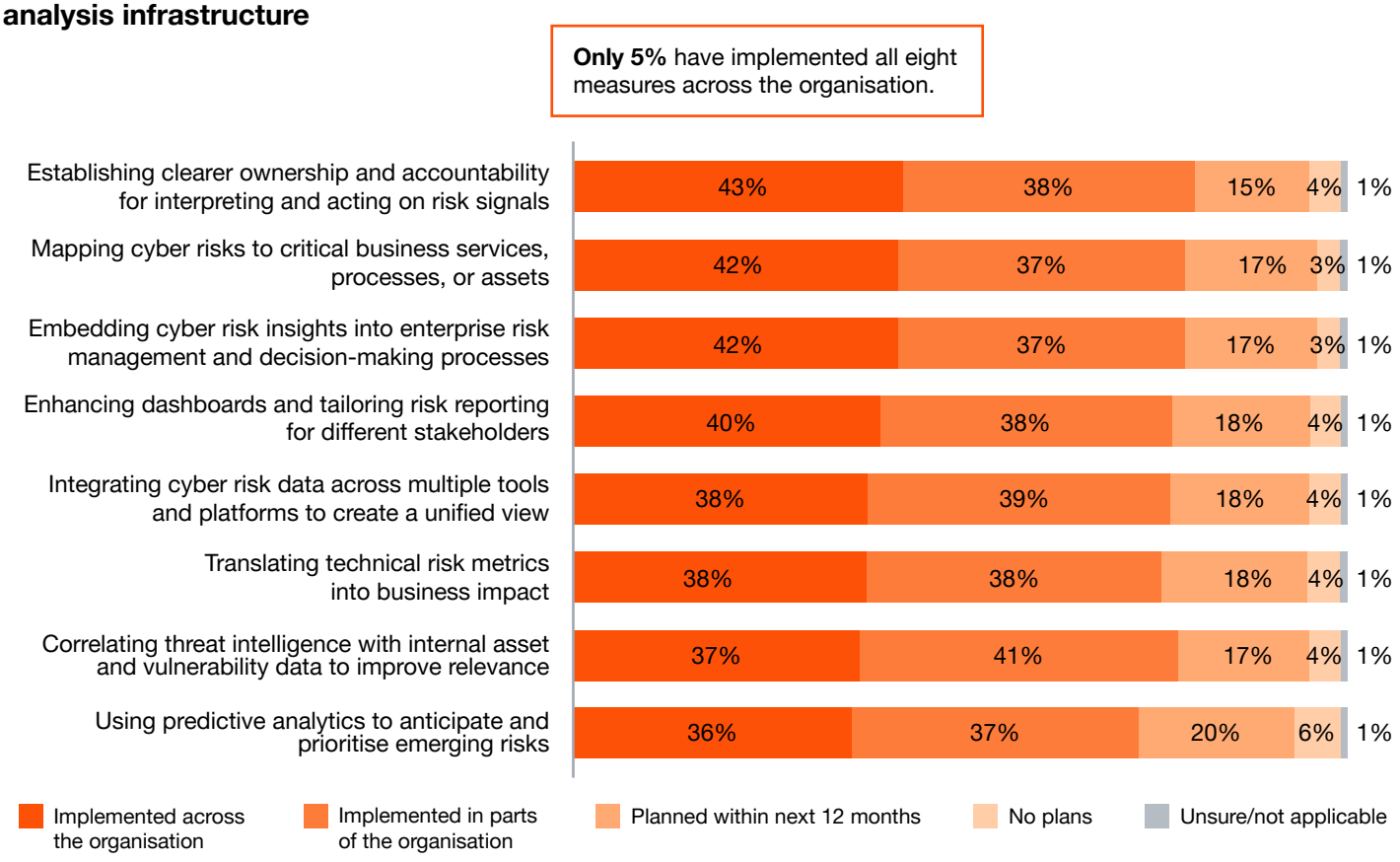
Phil Venables
Partner, Ballistic Ventures

Intelligence isn't leading to action...yet

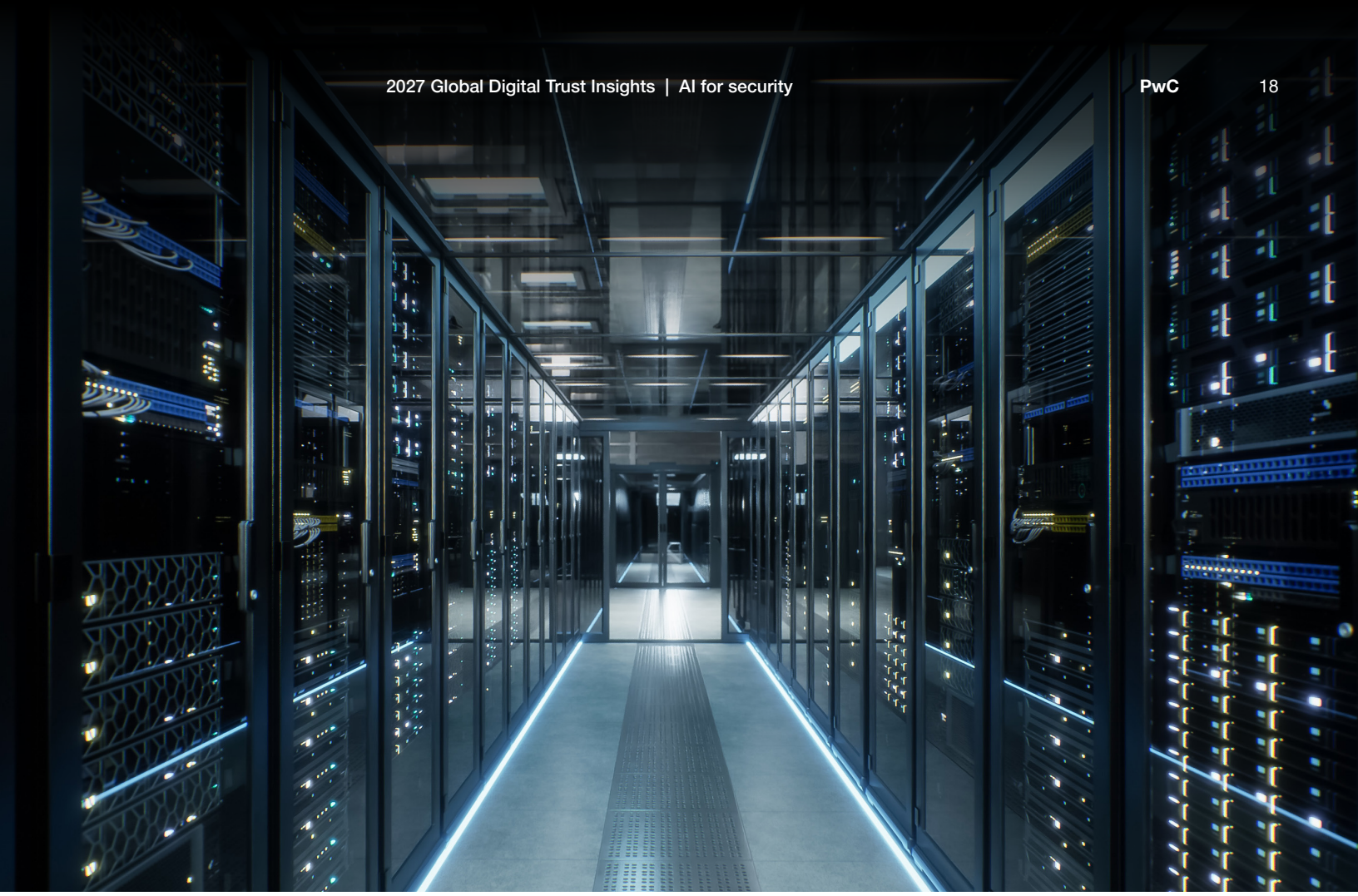
Context turns data into business insight. Organisations are implementing a range of capabilities, either in parts of the organisation or across it, to better contextualise cyber risk. These range from mapping cyber risks to critical business services (79%), to establishing ownership (81%), to integrating cyber risk data across multiple tools and platforms to create a unified view (77%).

But fewer than half have implemented any individual capability across the organisation. Just 42% have embedded cyber risk insights into enterprise risk management, while only 36% use predictive analytics to anticipate and prioritise risks. More concerning, only 5% have implemented all eight measures.

Measures for improving how cyber risk data is contextualised and incorporated into analysis infrastructure



Q13. To what extent has your organisation implemented any of the following measures to improve how cyber risk data is contextualised and incorporated into your analysis infrastructure for better decision-making?
Base: Chief AI officer, CIO, CISO, CSO, CTO, and director/VP/head equivalent, CDO, Chief Counsel, CIRO, CRO or Risk Director respondents (2151)
Source: PwC 2027 Global Digital Trust Insights



03

AI for security

Unlocking AI's defensive potential

No. 1

priority for using AI for cyber defence is threat detection and alerting

Only

22%

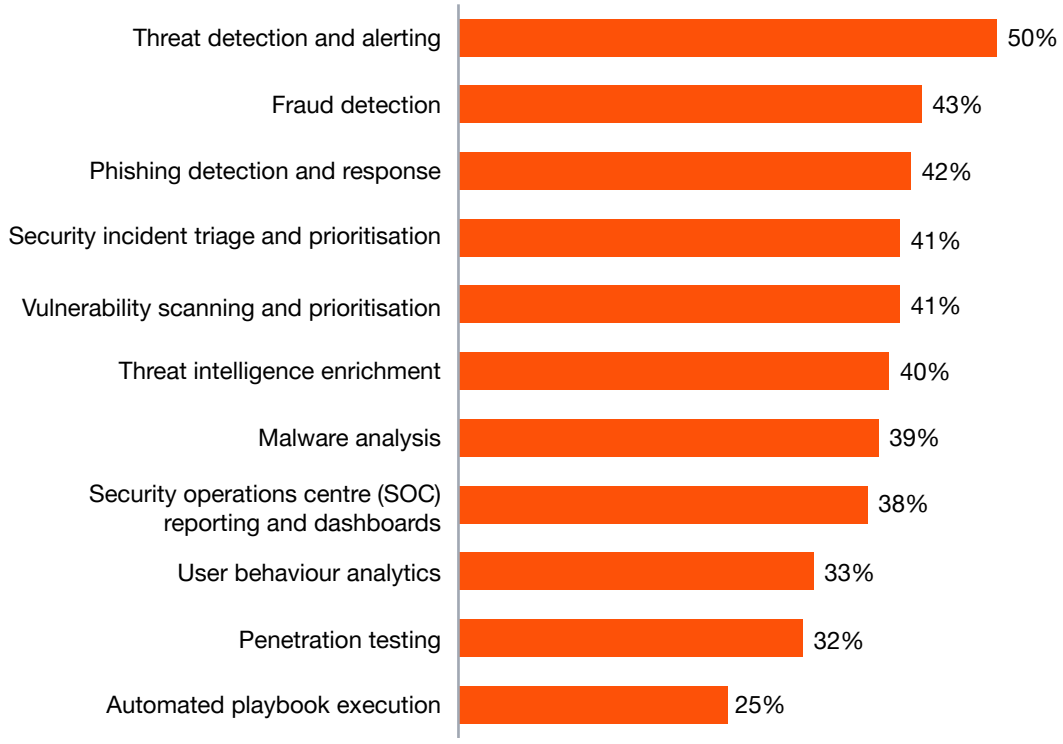
would authorise fully autonomous execution by AI agents for cyber defence without human approval

55%

say reliability and maturity concerns with current AI technology is a top barrier to increasing AI agent autonomy for security operations

The top defence against cyber attacks may be AI itself. With AI emerging as the top cyber investment priority, security leaders are deploying it first where speed and scale matter most. Half (50%) ranked threat detection and alerting among their top priorities, followed by fraud detection (43%) and phishing detection and response (42%). As cyber attacks accelerate beyond human speed, AI is becoming an essential force multiplier for security teams.

Priority areas for using AI in cyber defence in the next 12 months
(% that ranked in their top 5 priorities)



Q11. In which areas is your organisation prioritising AI for cyber defence over the next 12 months?
Base: Chief AI officer, CIO, CISO, CSO, CTO, and director/VP/head equivalent respondents (1819)
Source: PwC 2027 Global Digital Trust Insights

Ramping up to fully autonomous AI agents

The journey to using fully autonomous AI agents for cyber defence will happen in stages. While 22% would authorise AI agents to fully execute defensive manoeuvres without human approval, most are taking a more measured approach. More than one-third (38%) would permit partial autonomy, while 36% prefer human-led execution with AI support across all actions.

Routine tasks are the natural starting point. Organisations are most comfortable authorising autonomous agents for well-defined, repeatable activities such as threat intelligence enrichment and correlation (49%), phishing email quarantine or deletion (47%), and malware removal and system remediation (46%). As confidence grows, autonomy is likely to expand, but for now, security leaders are drawing clear boundaries around where AI can act independently.

Confidence in authorising autonomous AI agents to execute cyber defence actions without human approval



Q18. Which statement best reflects your level of confidence in authorising autonomous AI agents to execute cyber defence actions without human approval?
Base: All respondents (3934)
Source: PwC 2027 Global Digital Trust Insights

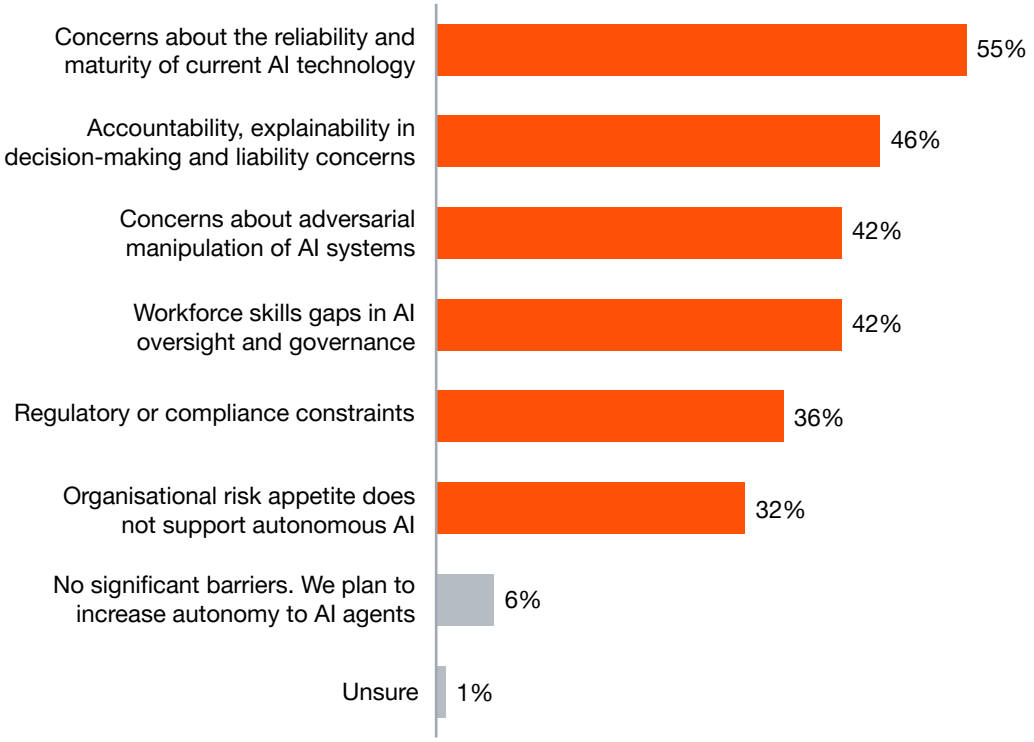
Trust in autonomous agents must be earned

Security teams are searching for ways to keep pace with threats. AI agents offer the promise of faster, more scalable cyber defence, but organisations are cautious about authorising these agents to act independently. More than half (55%) rank reliability and maturity of AI technology among their top three barriers to broader adoption of autonomous agents, while 46% cite accountability and explainability in AI decision-making.

The barriers extend beyond the technology itself. Nearly half of CISOs (44%) identify workforce skills in AI oversight and governance as one of their top barriers to increasing AI agent autonomy. Compared with the broader respondent population, CISOs appear more likely to recognise that successful deployment depends on having the right people in place to oversee it. Agents produce probabilistic output, so their autonomy should be governed by what stands between the agent and the consequence. Where an outcome should be correct every time, the agent's output should pass through a control the agent cannot influence, such as review, an approval workflow, or validation by another system before it takes effect.



Barriers to increasing AI agent autonomy for security operations
(% that ranked in their top 3 barriers)



Q20. What is preventing your organisation from increasing AI agent autonomy for security operations?
Base: All respondents (3934)
Source: PwC 2027 Global Digital Trust Insights



04

Leadership, talent, and governance

A foundation for cyber resilience

Only

47%

'strongly agree' that cyber risk is a standing agenda item for boards

33%

have established dedicated AI roles

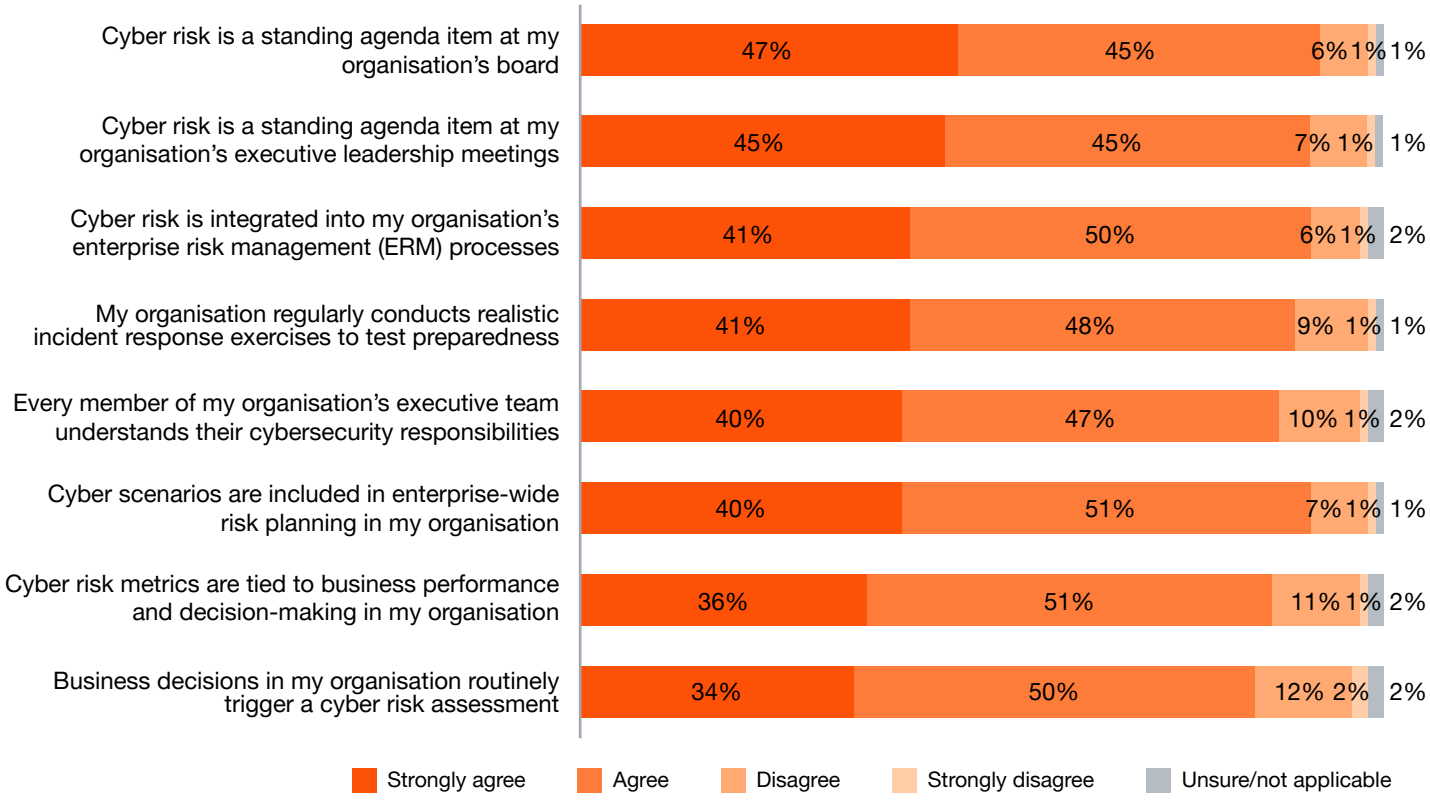
Top 2

priorities for managed services are AI and cloud

The core practices for governing cyber risk are largely in place. Roughly nine in 10 leaders agree that practices like board oversight, executive accountability, and enterprise risk integration are in place. That's progress compared to years past. But far fewer strongly agree that these capabilities are embedded in how the organisation operates.

Fewer than half strongly agree that cyber risk is a standing agenda item at the board level (47%) or at executive leadership meetings (45%), the strongest levels of agreement among the practices surveyed. There are even lower levels of agreement around business decisions routinely triggering cyber risk assessments and having cyber risk metrics tied to business performance. This suggests that while organisations have broadly adopted the practices needed to govern cyber risk, embedding them into day-to-day leadership and business decision-making is still a work in progress.

Treatment of cyber risk



Q23. To what extent do you agree or disagree with the following statements?
Base: All respondents (3934)
Source: PwC 2027 Global Digital Trust Insights

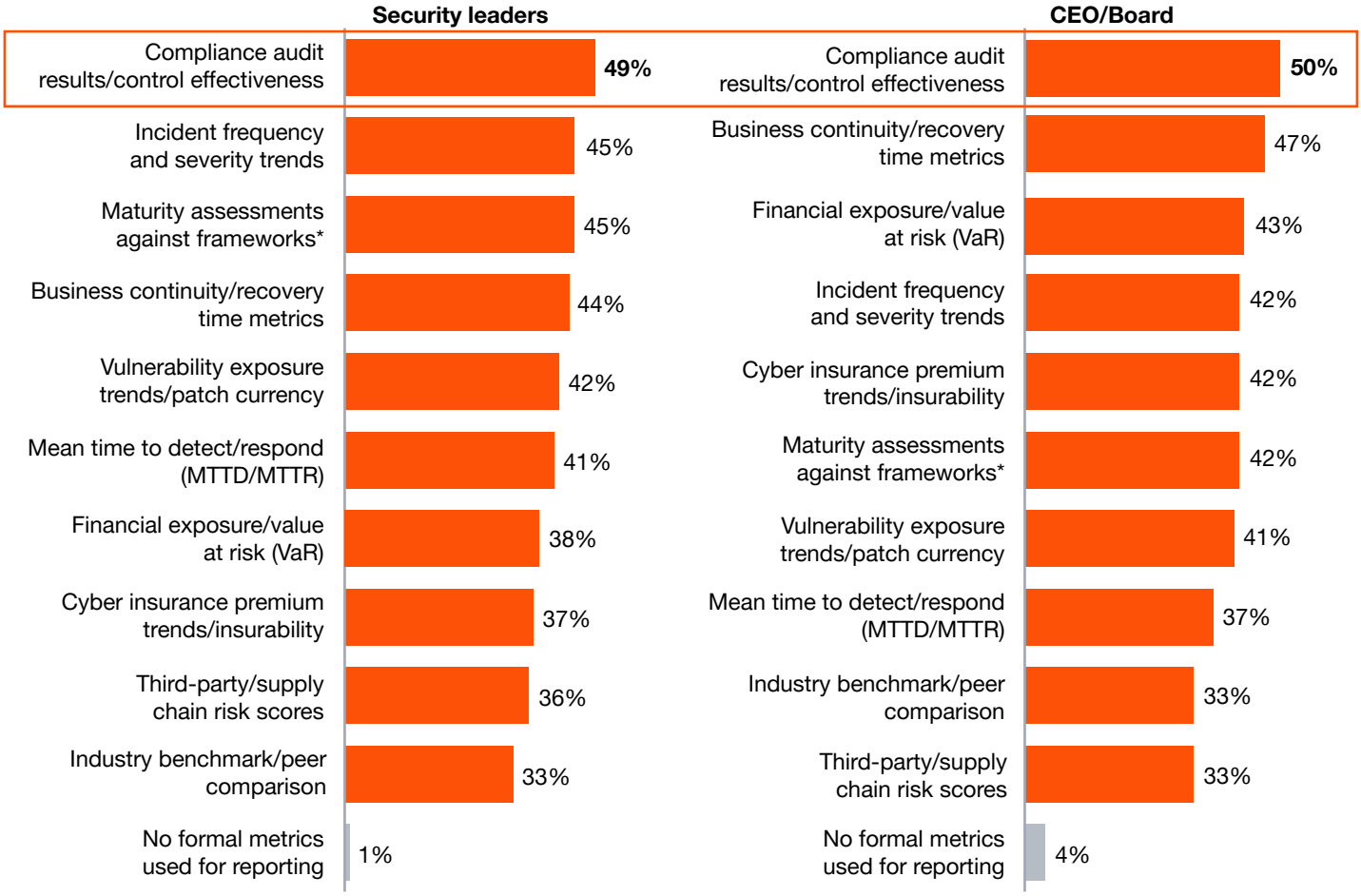
Measuring cyber success takes more than one metric

How do you know your cyber strategy is working? Security leaders, together with CEOs and the board, are largely aligned on the metrics that demonstrate whether cyber strategy is reducing risk. Compliance audit results and control effectiveness ranked highest for security leaders (49%) and CEOs and the board (50%), but the margins are narrow. Among security leaders, incident trends and maturity against frameworks also ranked highly (45% each). Among CEOs and the board, business continuity and recovery metrics took the second spot (47%). This reinforces compliance as a baseline, but demonstrating cyber effectiveness requires measuring beyond it.

This alignment on metrics creates a common foundation for governance and investment decisions, but it also highlights an important gap. While business continuity and recovery rank among top measures of cybersecurity success, only 39% of security, risk, and operations leaders have fully formalised and integrated continuity plans. Agreeing about what matters is a good first step. Operationalising it is the next challenge.



Most effective metrics to demonstrate that cyber strategy is reducing enterprise risk
(% that ranked in their top 5 metrics)



*(NIST CSF, ISO 27001, CIS)

Q24a. Which of the following metrics are the most effective in demonstrating to your board and executive leadership that your cyber strategy is reducing enterprise risk?
Base: Chief AI officer, CIO, CISO, CSO, CTO, and director/VP/head equivalent respondents (1819)
Q24b. Which of the following metrics are the most effective in demonstrating to [you and the CEO/Board] that your cyber strategy is reducing enterprise risk?
Base: Board, CEO respondents (720)
Source: PwC 2027 Global Digital Trust Insights

Responsible AI requires dedicated ownership

Building AI that is secure, resilient, and trusted by design requires clear accountability for AI governance and AI risk management, but no single ownership model has emerged. One-third (33%) of CEOs and security and risk leaders have already established dedicated AI roles, including chief AI officer or AI board. Others point to existing technology or cybersecurity teams or no single owner at all: 29% identify the CIO, CTO, or technology function; 17% the CISO or cyber function; and 11% say accountability is shared across multiple functions.

Clearly assigned accountability may also help organisations move beyond today's trust barriers. As security teams expand the use of AI for cyber defence, including autonomous AI agents, knowing who owns AI governance and AI risk management can provide the structure needed to build confidence and manage risk appropriately.

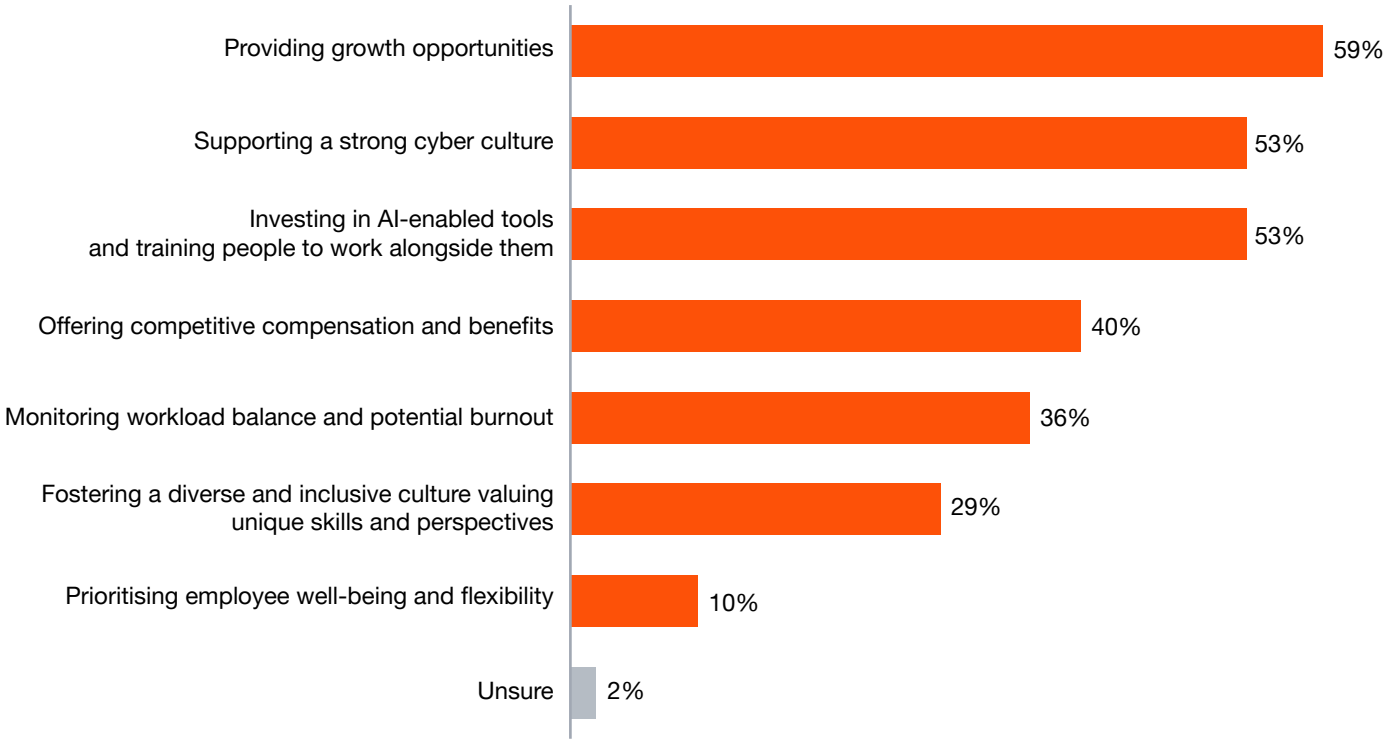
Preparing talent for an AI-enabled future

The cybersecurity skills gap remains a challenge. To retain employees, organisations place growth opportunities (59%), a strong cyber culture (53%), and AI-enabled tools and training (53%) among their top priorities. The emphasis is on development.

Traditional retention levers rank lower. Competitive compensation and benefits (40%), managing workload and burnout (36%), and prioritising well-being and flexibility (10%) rank well below opportunities for growth and AI enablement.

The results reflect a broader shift happening across cybersecurity. As AI becomes embedded in security operations, organisations appear to be placing greater emphasis on helping employees work alongside AI rather than on traditional retention strategies. This underscores how quickly AI is reshaping both security operations and workforce strategy. Yet capability gaps extend beyond AI. A lack of skills and resources remains the biggest challenge to securing operational technology and industrial systems.

Priority strategies to support professional development and retention of cybersecurity talent in the next 12 months (% that ranked in their top 3 priorities)



Q26. Which of the following strategies are you prioritising over the next 12 months to support the professional development and retention of your cybersecurity talent?
Base: All respondents (3934)
Source: PwC 2027 Global Digital Trust Insights

"To be successful in the era of AI, we need to be able to defend at machine speed."

Matt Rowe
Chief Security Officer, Lloyds Banking Group

Managed services have become essential

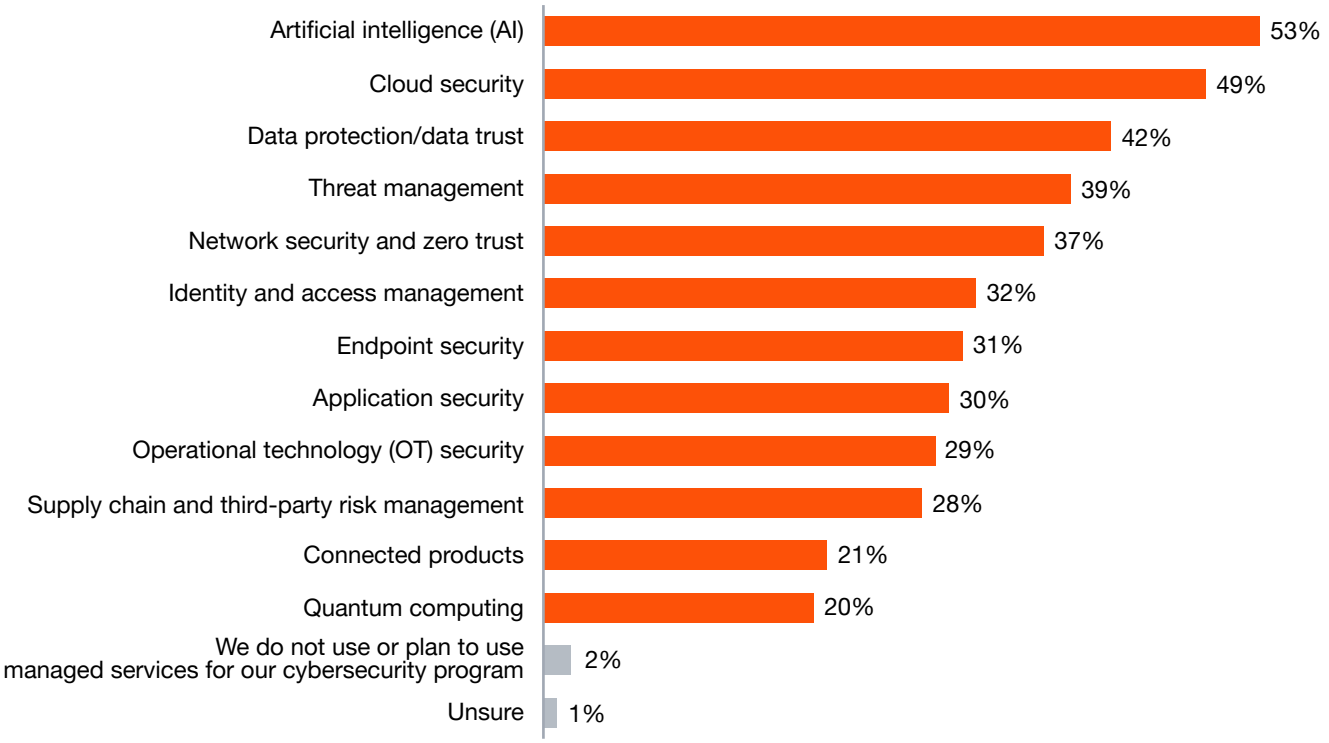
The survey tells a remarkably consistent story. AI and cloud security are the threats organisations feel least prepared to address. They're also the leading areas for cyber investment and use of managed security services. Security leaders rank AI (53%), cloud security (49%), data protection and trust (42%), and threat management (39%) among their top priorities for managed services over the coming year.

As in last year's survey, AI and cloud security topped the list.

This signals that organisations recognise the need for specialised partners that can provide a mix of talent, technology, and strategy to help them defend and adapt in a dynamic digital environment.



Priority areas for cybersecurity programs when using managed services in the next 12 months
(% that ranked in their top 5 priorities)



Q17. Which, if any, of the following areas of your cybersecurity programs is your organisation prioritising to use managed services over the next 12 months?
Base: Chief AI officer, CIO, CISO, CSO, CTO, and director/VP/head equivalent respondents (1819)
Source: PwC 2027 Global Digital Trust Insights



C-suite playbook

05 What leaders can do to keep pace in a dynamic digital world

This year's survey shows cyber risk being reshaped by geopolitical volatility, rapid advances in AI, and exposure that travels through interconnected ecosystems. These forces upend long-held assumptions about cybersecurity and what it takes for organisations to be resilient.

Organisations are increasing cyber investment, particularly in AI and cloud, but foundational gaps in data protection, operational continuity, and cyber risk management remain.

Even well-prepared organisations should rethink how to close the gaps that could disrupt business today while building the connected capabilities needed to adapt securely and create value.

This playbook sets out practical priorities leaders can act on together to strengthen cyber foundations and help build an **intelligent enterprise**—one where strategy, technology, and operations work as one, security is built in, and trusted data supports smarter, faster decisions.



Strengthen cyber governance, accountability, and risk decision-making

Cyber risk may have a seat at the leadership table, but it's not yet consistently embedded in how organisations make decisions. Stronger governance requires clear accountability, and leaders should be equipped with meaningful information to weigh risk alongside business priorities.

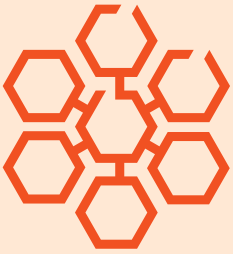
Strengthen the foundations

- **CEO:** Put cyber risk on every leadership and board meeting agenda and make it a regular part of strategic and operating discussions. Make cybersecurity a shared C-suite responsibility with clear accountability for cyber risk beyond the CISO.
- **CISO/CSO:** Make cyber risk a shared business responsibility by establishing governance that creates clear C-suite and board accountability and turns technical signals into business-focused reporting.
- **CRO:** Integrate cyber risk into enterprise risk management so it's evaluated alongside financial, operational, and strategic risks.
- **CFO:** Quantify cyber risk in financial terms to inform investment decisions, risk appetite, and enterprise planning.
- **Chief data officer/chief digital officer/chief AI officer:** Define enterprise capabilities and control objectives for how data is securely created, transformed, stored, accessed, and consumed.

Make your enterprise smarter

- **CEO:** Embed cyber insights into enterprise decision-making so leaders can anticipate change and prioritise risk.
- **CRO:** Connect cyber intelligence with enterprise risk, operational data, and financial data to give leaders a more complete view of changing exposure.
- **CFO:** Connect financial, operational, and risk data to give leaders a clearer view of investment priorities and enterprise exposure.

- **CISO/CSO:** Translate cyber risk insights into business-focused reporting so enterprise leaders can factor exposure, readiness, and resilience into strategic and operational decisions.
- **Chief data officer/chief digital officer/chief AI officer:** Lead the shift from governance as bureaucracy to strategic enabler, with clearly defined semantics, lineage, and controls that enable safe, autonomous AI actions.



Protect critical operations and build cyber resilience

Cyber resilience is ultimately tested by whether the business can operate through disruption. Continuity planning needs to move from a preparedness exercise to an integrated enterprise capability. Start by defining your **minimum viable company**—the smallest set of capabilities needed to keep your organisation operating through disruption—then build and test recovery plans around the technology and third parties that support it.

Strengthen the foundations

- **CISO/CSO:** Maintain visibility across critical assets, operational technology (OT) environments, third-party access paths, and legacy systems so teams can see where disruption could reach high-value operations, and create strong perimeters between IT and OT networks to prevent cross-contamination and lateral threat movement.
- **COO:** Embed cybersecurity into operational resilience, business continuity, and crisis management so the organisation can recover quickly when disruption occurs. Map critical business services, sites, suppliers, workforce dependencies, and technology services, including their cyber risk exposure, that support customer delivery, safety, revenue continuity, and regulatory commitments.
- **CRO:** Stress-test operational resilience using cyber scenarios that challenge critical business services, dependencies, and recovery assumptions.
- **CFO:** Improve resilience of financial operations by identifying critical processes, dependencies, and recovery requirements.
- **CEO:** Insist on continuity planning so the business is prepared to operate and recover when cyber disruption occurs.

Make your enterprise smarter

- **COO:** Secure intelligent workflows that bring AI, data, and human decision-making together while limiting operational exposure. Define human oversight, exception handling, and manual fallbacks for automated decisions that affect customers, employees, transactions, or critical services.
- **CRO:** Model interconnected cyber scenarios to understand how disruption could cascade across operations, technology, suppliers, and markets.
- **CEO:** Build adaptive operations that evolve with new threats, technologies, and business priorities.
- **CISO/CSO:** Use AI and automation to unify security signals, detect threats faster, reduce manual effort, and help teams respond at machine speed.



Secure data, AI and emerging technology

AI trustworthiness depends heavily on the underlying data, but data protection remains a persistent gap. This gap matters more as organisations expand their use of AI for cyber defence and consider giving AI agents greater autonomy. Building trust in AI starts with a foundation that can be trusted.

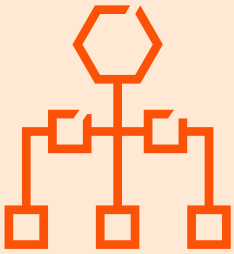
Strengthen the foundations

- **CISO/CSO:** Protect critical and sensitive data with consistent discovery, classification, access controls, and monitoring across the enterprise.
- **CTO/CIO:** Protect data across the technology estate through consistent controls, access management, and continuous monitoring.
- **Chief data officer/chief digital officer/chief AI officer:** Map critical data flows across the organisation, focusing on high-value, high-velocity, and highly sensitive data in coordination with the CISO. Establish privacy controls that scale with AI adoption, including consent management, data minimisation, and privacy-by-design.
- **CFO:** Prioritise data quality for financial disclosures, regulatory reporting, and executive KPIs.
- **CRO:** Map data risks across the business processes, reports, and KPIs that matter most.

Make your enterprise smarter

- **CISO/CSO:** Secure AI data pipelines and model environments by applying human and non-human access controls, monitoring, privacy safeguards, and security requirements in partnership with data, digital, and AI leaders.
- **CTO/CIO:** Build responsible AI into delivery so governance, security, and risk controls scale alongside AI adoption.
- **CEO:** Set expectations for trusted AI adoption with clear ownership, governance, and accountability for managing AI-related risk.
- **CFO:** Measure AI value alongside AI risk so investment decisions account for expected returns, exposure, and cost of controls.
- **Chief data officer/chief digital officer/chief AI officer:** Govern AI training data to verify that it is curated and ethically sourced, with AI pipelines accessing enterprise data products and model outputs feeding back into secure, governed environments. Build explainability into AI systems so risk, compliance, and business leaders can audit decision logic, investigate errors, and respond to regulatory inquiries.





Manage ecosystem, third-party, and technology concentration risk

Cyber risk travels across the enterprise ecosystem. Cloud providers, technology platforms, suppliers, and other third parties can turn a vulnerability or disruption elsewhere into a business risk. Resilience depends on understanding those dependencies and where concentrations of risk could amplify impact.

Strengthen the foundations

- **CISO/CSO:** Identify concentrations of risk across cloud, third-party, supplier, and OT ecosystems that could create single points of failure or allow disruption to cascade across critical operations.
- **CTO/CIO:** Reduce cloud risk concentration through multi-cloud or hybrid cloud strategies and build greater redundancy for critical technology and data. Map technology dependencies so teams understand which systems, providers, and infrastructure must be restored first after disruption.
- **COO:** Review sourcing, vendor dependency, and embedded technology exposure as operational resilience issues, not only procurement or technology issues. Validate recovery assumptions with critical third parties that support priority operations, including vendors, logistics providers, managed services, cloud platforms, and infrastructure partners.
- **CRO:** Quantify geopolitical cyber exposure across critical operations, markets, and third parties vulnerable to state-sponsored attacks or disruption.

Make your enterprise smarter

- **CTO/CIO:** Engineer for interoperability and scale so data, AI, and applications operate as a connected system rather than isolated investments. Align modernisation roadmaps with zero-trust architecture, post-quantum cryptography, cloud migration, and AI-powered cyber tools.
- **CEO:** Connect ecosystem visibility to enterprise strategy so leaders can anticipate third-party risks and respond with greater confidence.

- **CFO:** Evaluate the economics of managed services against the cost and capability required to build and maintain specialised talent, technology, and capabilities internally.
- **CISO/CSO:** Assess vendor concentration risk as an attacker would by simulating the paths and shared infrastructure that could let a single incident cascade across seemingly independent vendors. Supplement third-party self-attestations with independent, always-on signals, such as attack surface scans, infrastructure fingerprinting, and news monitoring to verify actual vendor dependencies and catch risk in real time.



Use trusted technology and data to create enterprise value

Cybersecurity can do more than protect enterprise value—it can help create it. As organisations modernise technology and invest in AI, cloud, and data, security should be considered alongside business value from the start. The goal is an enterprise that can innovate and grow with confidence.

Strengthen the foundations

- **CTO/CIO:** Modernise legacy technology that creates security exposure, limits visibility, or slows the organisation's ability to respond to change. Build security into technology decisions from the start rather than adding controls after platforms, applications, and products are deployed.
- **CFO:** Prioritise cyber investments based on business exposure, resilience needs, and the potential financial impact of disruption.
- **CEO:** Reframe cybersecurity as a strategic capability tied to enterprise growth, innovation, resilience, and competitive position.
- **Chief data officer/chief digital officer/chief AI officer:** Verify the organisation has the right talent to execute at scale, including expertise in data modelling, data engineering, data architecture, data security, and data risk management.

Make your enterprise smarter

- **CTO/CIO:** Build the technology foundation for AI at scale by modernising cloud, data, applications, and architecture around connected enterprise needs. Move AI beyond isolated use cases by designing platforms and workflows that connect AI to business processes and decisions.
- **CEO:** Design a connected enterprise so leaders can make faster decisions, respond to change with greater confidence, and create value at scale.
- **CFO:** Invest in trusted data foundations that support reliable AI, financial reporting, and faster enterprise decision-making.
- **Chief data officer/chief digital officer/chief AI officer:** Build data products abstracted from applications and designed for enterprise-wide reuse, providing curated, governed, and well-documented assets. Enable self-service data delivery so business users, analysts, and product teams can find and consume data through controlled, governed APIs.



Build the model for human-and-agent operations

The intelligent enterprise will depend on people and AI agents working together through secure platforms, trusted data, and clearly governed workflows. Leaders should pair new capabilities with human accountability, workforce development, and controls that preserve quality, resilience, and trust as autonomy increases.

Strengthen the foundations

- **COO:** Redesign AI-enabled workflows with named human owners, intervention points, exception queues, manual fallbacks, and procedures for operating when agents or models are unavailable or compromised.
- **Chief data officer/chief digital officer/chief AI officer:** Implement explainability, lineage, and audit records sufficient to reconstruct material AI decisions, investigate errors and respond to customer, regulatory and internal-review questions.
- **CIO/CTO:** Provide secure platforms, observability, access controls, and revocation mechanisms that allow people and agents to work together without expanding authority by default.
- **All C-suite leaders:** Define priority capability gaps in AI security, cloud, data, OT, resilience, and agent oversight, and maintain workforce plans covering development, recruitment, role redesign, and succession.

Make your enterprise smarter

- **CISO/CSO and CIO/CTO:** Equip teams with AI-enabled tools and training, define approved uses and human-review requirements, and measure improvements in productivity, quality, control effectiveness, and response time.
- **CISO/CSO:** Use strategic partners to access scarce expertise and accelerate transformation while retaining ownership of risk, architecture, and decision rights.
- **Chief data officer/chief digital officer/chief AI officer:** Build data engineering, architecture, security, and governance skills needed to operate trusted data and AI products at scale with clear service-level expectations.
- **CEO:** Consider career pathways, rotational assignments, and executive sponsorship to strengthen cybersecurity culture, improve retention, and develop leaders able to operate across technology, risk, and business functions.



About this report

The 2027 Global Digital Trust Insights survey captured the views of 3,934 business and technology leaders and was conducted in May through July 2026.

More than one-third of the executives (36%) 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 (19%); tech, media, and telecom (20%); retail and consumer markets (16%); healthcare (10%); energy, utilities, and resources (10%); and government and public services (3%).

Respondents are based in 71 countries. The regional breakdown of responses is Western Europe (32%), North America (26%), Asia Pacific (18%), Latin America (12%), Central and Eastern Europe (4%), Africa (5%), and the Middle East (3%).

The Global Digital Trust Insights survey was previously known as the Global State of Information Security Survey (GSISS). Now in its 29th year, it's the longest-running annual survey on cybersecurity trends. It's also one of the largest surveys in the cybersecurity industry and the only one that draws participation from senior business leaders, not just security and technology leaders.

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

Contact us

Avinash Rajeev
Global and APA Cyber Data & Tech Risk Leader
avinash.rajeev@pwc.com - LinkedIn

James Rashleigh
EMEA Cyber Data & Tech Risk Leader
james.m.rashleigh@pwc.com - LinkedIn

Morgan Adamski
US Cyber Data & Tech Risk Leader
morgan.m.adamski@pwc.com - LinkedIn

© 2026 PwC. All rights reserved. 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. This content is for general purposes only, and should not be used as a substitute for consultation with professional advisors.