



Bridging the gaps to cyber resilience: The C-suite playbook

**Findings from the 2025 Global
Digital Trust Insights**

Findings from the 2025 Global Digital Trust Insights

2%

Only 2% have implemented cyber resilience actions across their organisation in all areas surveyed

50%

Under 50% of CISOs are involved to a large extent in key business activities

13%

point gap in confidence between CISO/CSOs and CEOs regarding compliance with AI and resilience regulations

With the attack surface continuing to expand through advances in AI, connected devices and cloud technologies and the regulatory environment in constant flux, achieving cyber resilience at an enterprise level is critical.

Yet despite widespread awareness of the challenges, significant gaps persist. To safeguard their organisations, executives should treat cybersecurity as a standing item on the business agenda, embedding it into every strategic decision and demanding C-suite collaboration.

PwC's 2025 Global Digital Trust Insights survey of 4,042 business and tech executives from across 77 countries revealed significant gaps companies must bridge before achieving cyber resilience.

■ Gaps in implementation of cyber resilience:

Despite heightened concerns about cyber risk, only 2% of the executives say their company has implemented cyber resilience actions across their organisation in all areas surveyed.

■ Gaps in preparedness:

Organisations feel least prepared to address the cyber threats they find most concerning, such as cloud-related risks and third-party breaches.

■ Gaps in CISO involvement:

Fewer than half of the executives say their CISOs are involved to a large extent in strategic planning, board reporting and overseeing tech deployments.

■ Gaps in regulatory compliance confidence:

CEOs and CISO/CSOs have differing levels of confidence in their company's ability to comply with regulations, particularly regarding AI, resilience and critical infrastructure.

■ Gaps in measuring cyber risk:

Although executives acknowledge the importance of measuring cyber risk, fewer than half do so effectively, with only 15% measuring the financial impact of cyber risks to a significant extent.

All of this points to the need for better C-suite collaboration and strategic investment to strengthen cyber resilience. By addressing these gaps and making cybersecurity a business priority, executives can bridge to a more secure future.

CISOs can help drive this outcome by sharing tech-enabled insights and by explaining cyber priorities in business terms (cost, opportunity, risk).



Table of contents

4	<u>Navigating cyber threats: Establishing a shared vision for preparedness</u>
7	<u>GenAI and emerging tech: Balancing opportunity and risk</u>
10	<u>A highly regulated cyber world: Are companies really ready?</u>
13	<u>Unlocking the potential of cyber risk quantification: What's holding organisations back?</u>
16	<u>Investing in resilience, building trust</u>
19	<u>Is your cyber strategy and leadership driving real resilience?</u>

Navigating cyber threats: Establishing a shared vision for preparedness



66%

of tech executives rank cyber as the highest risk for mitigation, compared to 48% of business executives

42%

of executives rank cloud-related threats as their most concerning cyber threat

Top 2

Cloud and connected product attacks are what security executives feel least prepared to address

While the cybersecurity landscape continues to evolve, organisations are struggling with increasingly volatile and unpredictable threats. An expanding attack surface — spurred by growing reliance on cloud, AI, connected devices and third parties — demands an agile, enterprise-wide approach to resilience. Aligning organisational priorities and readiness is essential for maintaining security and business continuity.

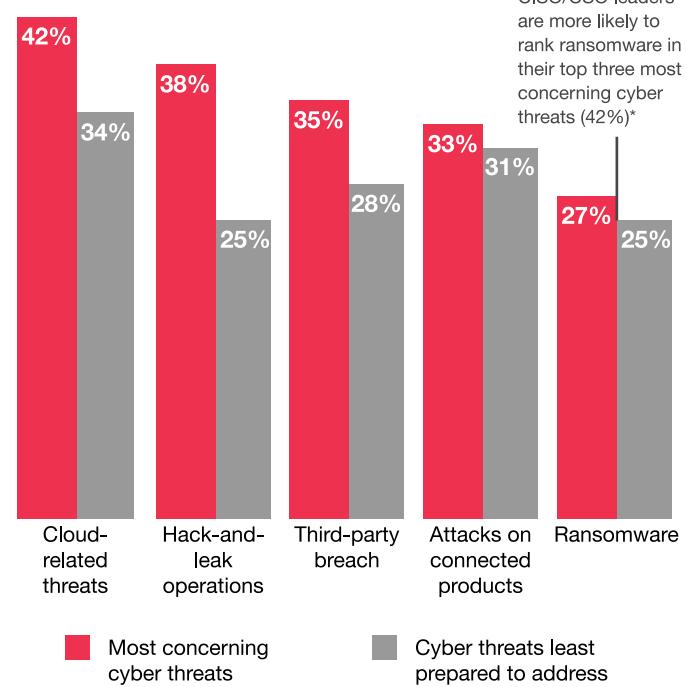
Unprepared for the most concerning threats

What worries organisations most is what they're least prepared for. The top four cyber threats found most concerning — cloud-related threats, hack-and-leak operations, third-party breaches and attacks on connected products — are the same ones security executives feel least prepared to address. This gap highlights the urgent need for better investments and stronger response capabilities.

Additionally, a perception gap exists between security executives and the rest of the organisation, with CISOs and CSOs more likely to rank ransomware among their top three most concerning threats. This may reflect their role, as ransomware is more central to cyber/IT duties and those in that function likely understand the vulnerabilities better than their business peers. This further reinforces the importance of better information-sharing across leadership teams to create alignment on priorities.

Cyber threat concern vs preparedness

(showing % ranked 1-3)



CISO/CSO leaders are more likely to rank ransomware in their top three most concerning cyber threats (42%)*

*As compared to 27% globally
Q2. 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)? (Ranked in top three) Base: All respondents= 4042
Q3. Over the next 12 months, which of the cyber threats do you think your organisation is least prepared to address? (Ranked in top three) Base: Security leaders and CFO respondents= 1951
Source: PwC 2025 Global Digital Trust Insights

Wake-up call

A threat-informed cyber investment strategy is essential. Prioritise investments in the most pressing cyber risks and take a closer look at where resources are being applied in terms of people, process and defence capabilities.

The strategic divide: Business and tech priorities

Business executives and tech executives prioritise different risks. While business executives are more concerned with inflation, tech executives rank cyber risks as their top priority — likely due to their proximity to the cyber threat landscape. Even so, nearly half of business executives still rank cyber risks among their top three concerns, underscoring its critical importance. This shared concern represents an opportunity for CISOs to connect the cyber agenda to the business agenda.

Risk mitigation priorities for business vs tech leaders

(showing % ranked 1-3)

Inflation



Digital and technology risks



Cyber risks



Business leaders

Tech leaders

Q1. Which of the following risks is your organisation prioritising for mitigation over the next 12 months? (Ranked in top three) Base: All respondents= 4042
Source: PwC 2025 Global Digital Trust Insights

Wake-up call

Business and tech executives — it's time to get aligned. Balance prioritisation of cyber risks with economic pressures to help safeguard assets and create resilience. Regular cross-functional assessments will keep your strategy and priorities in sync.

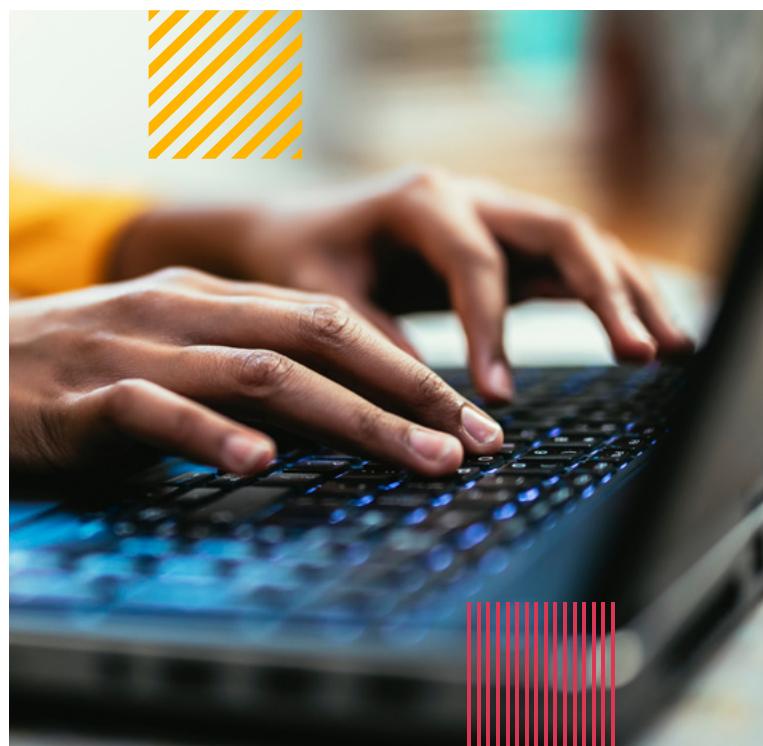
Global average data breach cost exceeds \$3 million

Over a quarter of executives tell us their most damaging data breach in the past three years cost their organisation at least \$1 million. This is somewhat lower than last year's survey across organisations of all sizes and in most regions and sectors. Overall, the average data breach is estimated at \$3.32 million.

Top performers — identified as those who responded that their organisation is more likely to demonstrate high quality cybersecurity practices on a usual basis — were less likely to experience any data breaches in the past three years. These top performers are typically from larger, high-growth organisations with cyber budgets expected to increase by 15% or more next year, indicating that cyber program maturity and funding correlate to better resilience.

“Don’t stop short on your journey for cybersecurity and resilience. Criminals and nation-state actors are becoming expert at finding unprotected seams: weak identity and access controls, unpatched devices and security misconfigurations.”

Rob Joyce, Cyber, Risk & Regulatory Senior Fellow, PwC US, former Special Assistant to the President & Acting Homeland Security Advisor



Wake-up call

Prioritise holistic risk mitigation strategies that encompass prevention, detection, response and recovery. Understand the broader impacts of a breach — beyond financial harm — to build true resilience.

Executive call-to-action

As organisations face a more sophisticated threat landscape, it's important for [executives across the C-suite](#) to take a proactive role in assessing both current and emerging risks. By aligning cybersecurity strategies with broader business objectives, executives can better prepare their organisations to manage risk and build resilience.

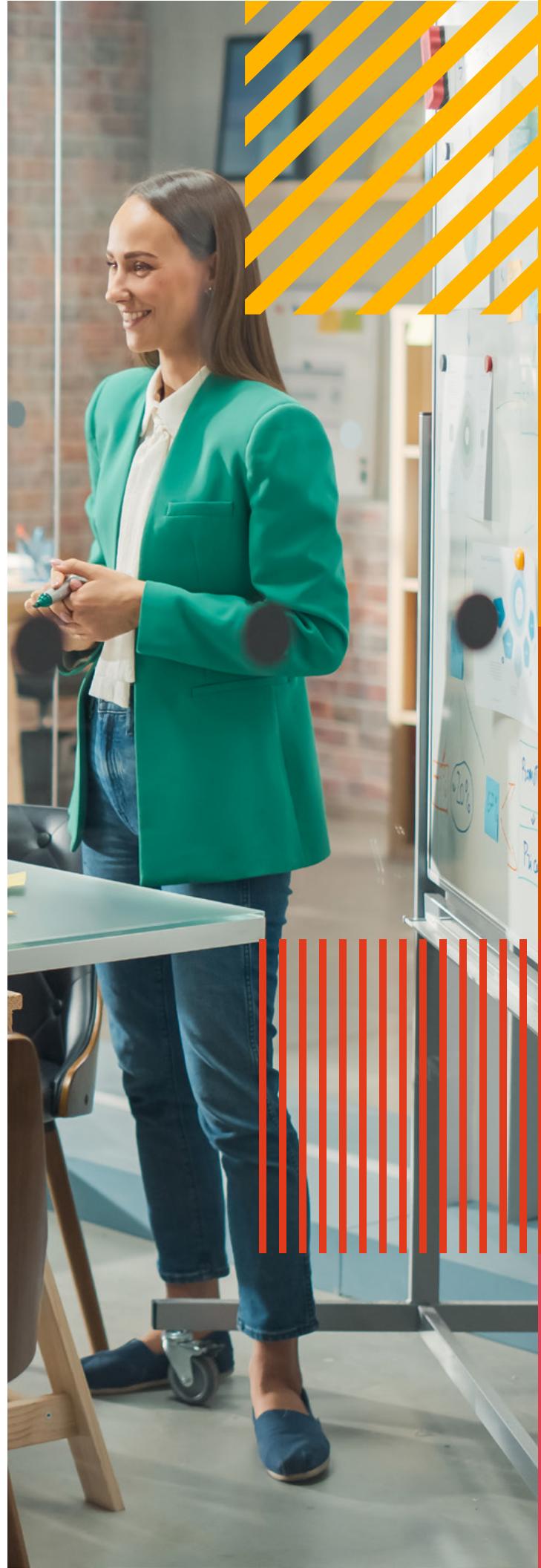
CISOs: Underscore to the rest of the C-suite the threats that jeopardise your business most, especially if investment efforts need to be shifted.

CIOs and chief technology officers (CTOs): Based on conversations with the risk executives, gauge how certain threats can damage information and infrastructure security at large and which threats pose the biggest barriers to resilience.

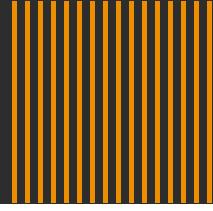
CFOs: Gain deeper insight from the CISO and CRO on the most critical cyber management and investment priorities.

CEOs: Meet regularly with the CRO and CISO to understand the threat vectors they're most concerned about. Make sure you're receiving regular reporting on current threat mitigation efforts.

Board: Understand the top cyber risks to the organisation and ask the tough questions of management. How are risks being mitigated? Do we have adequate plans and funding in place to proactively address risks and respond should an event occur?



GenAI and emerging tech: Balancing opportunity and risk



67%

of security executives say that GenAI has increased their attack surface over the last year

78%

have increased their investment in GenAI over the last 12 months

72%

have increased their risk management investment in AI governance

While the rapid advancement of generative AI (GenAI) is ushering in new opportunities across industries, it also presents cybersecurity risks. As organisations adopt GenAI and other emerging technologies, the C-suite should navigate more complex and unpredictable attack vectors, integration obstacles and the dual-edged nature of GenAI in both cyber defence and offence. Underlying these challenges are significant data and legal issues that can complicate the deployment and governance of GenAI.

“ Cybersecurity is predominantly a data science problem. It’s becoming imperative for cyber defenders to leverage the power of generative AI and machine learning to get closer to the data to drive timely and actionable insights that matter the most.”

Mike Elmore, Global CISO, GSK

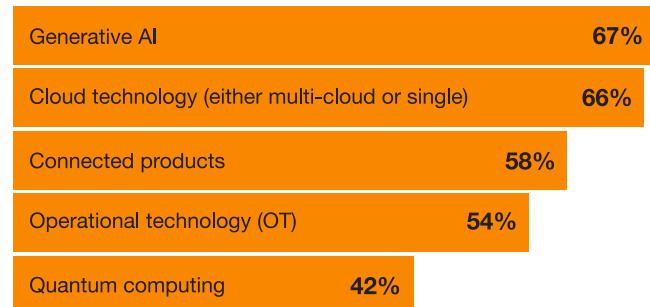
An evolving attack surface

Security executives report that GenAI (67%) and cloud technologies (66%) have expanded the cyber attack surface over the past year, making companies more vulnerable to sophisticated threats. GenAI can also reduce barriers to

entry for less sophisticated threat actors, enabling them to craft effective phishing attacks and deepfakes at scale. This aligns with the findings of our [27th CEO Survey](#), in which 64% of CEOs globally agreed that GenAI is likely to increase cybersecurity risk in their organisation. Use of GenAI also raises concerns about data integrity, privacy and compliance as companies deal with regulatory obligations that are still evolving.

Also expanding the attack surface are other technologies such as connected devices and operational technology (OT), which will affect industries such as manufacturing, healthcare and energy. As more devices become interconnected, securing these systems becomes harder. In addition, while quantum computing is still on the horizon, 42% percent of security executives report that it has already caused them to address vulnerabilities.

Technologies affecting the cyber attack surface*



*Showing combined percentage who selected ‘increase significantly’ or ‘increase slightly’ Q4. To what extent have the following technologies affected the cyber attack surface in your IT environment over the last 12 months? Base: Security leaders= 1762
Source: PwC 2025 Global Digital Trust Insights

Wake-up call

Continuous assessment of new vulnerabilities, investment in advanced security measures and fostering closer collaboration between technology, security, risk and legal teams are paramount. By staying prepared for these threats, companies can better safeguard critical assets and maintain stakeholder trust.

Leveraging GenAI for cyber defence: Opportunities and challenges

Although GenAI is increasing the cyber risk attack surface for most organisations, executives are also using that same technology for cyber defence. The top three ways they're leveraging GenAI include threat detection and response, threat intelligence and malware/phishing detection.

However, despite these opportunities, organisations face several obstacles when incorporating GenAI into their cyber defence strategies.

Difficulty incorporating with existing systems/processes (39%)

Lack of trust in GenAI by internal stakeholders (39%)

Inadequate internal controls and risk management (38%)

Lack of standardised internal policies governing its use (37%)

Wake-up call

GenAI can transform your cyber defences, but only if you overcome the challenges to integrate, trust and govern it effectively, applying Responsible AI practices. Otherwise, you risk falling behind in the arms race against threat actors.

GenAI leads in cyber investment priorities

Recognising the increased cyber risks, 78% of executives have ramped up their cyber investment in GenAI, particularly focusing on governance. This investment in GenAI underscores the importance of managing both its capabilities and risks.

Companies are also beginning to [invest in quantum preparedness](#). Although adoption remains years away, there's already a growing imperative to pursue quantum-resistant technologies and post-quantum security measures to combat future threats posed by this technology in the wrong hands.



Wake-up call

Investing in GenAI is just the start. Move the needle more by exploring the untapped potential of other technologies, including quantum-resistant solutions, to help your defences outpace evolving threats.

Executive call-to-action

As emerging technologies reshape the cybersecurity landscape, it's critical for executives across the C-suite to take an active role in guiding their organisations through both the opportunities and risks these innovations present.

CISOs: Help to drive standardisation across the technology estate to help integrate AI into cyber defences. Enforce access rights on a user-by-user basis to identify probable attack vectors.

CIOs and CTOs: Develop an AI impact assessment to educate business executives on where investment and implementation makes the most sense. Prepare your platforms for scalability as GenAI use grows.

CFOs: Work with the CISO on prioritising the security and confidentiality of financial data protection.

Chief data officers (CDOs): Enhance your data governance protocols and assess any data privacy risks against privacy laws and regulator guidance.

Chief legal officers (CLOs) and general counsel (GCs): Collaborate with other risk and compliance teams to guard against improper secondary uses of data and potential legal exposure.



Regulatory developments

A highly regulated cyber world: Are companies really ready?



96%

report that cybersecurity regulations have spurred them to increase their cyber investment in the last 12 months

78%

believe that regulations have helped to challenge, improve or increase their cybersecurity posture

13%

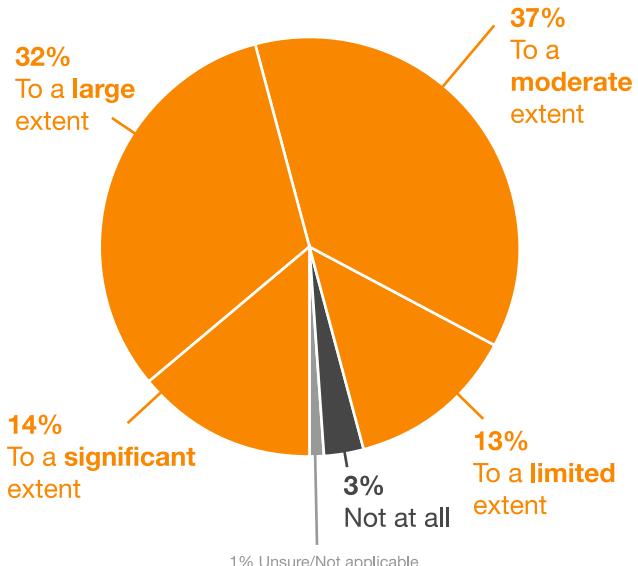
point gap in confidence between CISO/CSOs and CEOs regarding compliance with AI and resilience regulations

Regulatory frameworks are asking companies to swiftly comply with a growing array of requirements. A surge of new regulations — DORA, Cyber Resilience Act, AI Act, CIRCIA, Singapore Cybersecurity Act, etc. — underscores the urgency for organisations to align their practices to these heightened expectations. As businesses navigate these demands, they face a critical gap in confidence between CISO/CSOs and CEOs regarding their ability to achieve full compliance. Addressing these challenges is essential to building a resilient and compliant cybersecurity posture that can withstand both regulatory scrutiny and emerging threats.

Cyber regulations are driving positive change

Cyber regulations are proving to be a major driver for cybersecurity investment, with 96% of executives acknowledging that regulatory requirements have spurred them to enhance their security measures. Moreover, 78% believe that regulations have helped to challenge, improve or increase their cybersecurity posture. This indicates that, despite the difficulties of compliance, regulations are serving to further mature cybersecurity capabilities across industries.

Impact of cybersecurity regulations on increasing cybersecurity investment



Q16. To what extent, if at all, have cybersecurity regulations increased your organisation's cybersecurity investment over the last 12 months? Base: Security leaders and CFO respondents= 1951
Source: PwC 2025 Global Digital Trust Insights

Helpful impact on organisations

Cybersecurity regulations **helped 78%** of organisations

Impact Statement	Percentage
challenged our organisation to strengthen current cyber risk management program, processes and governance approaches	24%
helped establish guardrails for technology innovation and transformation efforts	20%
helped become more resilient by mandating an industry-wide framework	19%
led us to consider cyber managed services to address regulatory requirements	15%

Q17. Which one statement, if any, best reflects the impact of new cybersecurity regulations on your organisation over the last 12 months? Base: All respondents= 4042
Source: PwC 2025 Global Digital Trust Insights

Wake-up call

Organisations that embrace regulatory requirements tend to benefit from stronger security frameworks and a more robust posture against emerging threats. Compliance shouldn't be viewed as a box-ticking exercise but as an opportunity to build long-term resilience and trust with stakeholders.

Confidence gap: CISOs feel less certain than CEOs about cyber compliance

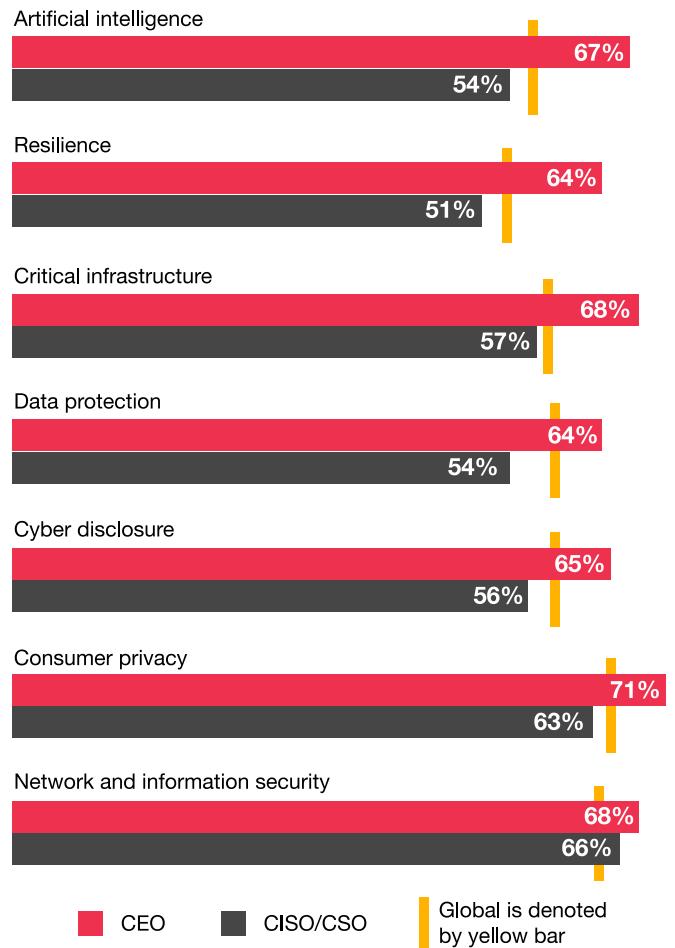
Despite the belief that cyber regulations are helping the organisation, there's a significant difference between CEO and CISO/CSO confidence in their ability to comply with these regulations. The biggest gaps involve compliance with AI, resilience and critical infrastructure requirements. CISOs, who are on the front lines of cybersecurity, are less optimistic than CEOs about their organisation's ability to meet these regulatory requirements.

Because CISOs are more attuned to the day-to-day operational difficulties, resource constraints and potential vulnerabilities that can hinder cyber compliance, it's vital that they more effectively communicate these risks to the leadership team. What's preventing them? Potential obstacles include barriers to CISO participation in strategic decisions and an inability to justify the amount of cyber risk investment needed.



Confidence in organisation's regulation compliance

Showing % high confidence for CEO vs CISO/CSO



Q15. How confident are you in your organisation's ability to be in compliance with the following types of regulations that may apply to the geographic area(s) in which your organisation operates? Base: All respondents = 4042
Source: PwC 2025 Global Digital Trust Insights

Wake-up call

Bridging this confidence gap requires better alignment and communication between security executives and the C-suite. CEOs should make sure that CISOs aren't only heard but also have the resources and support necessary to meet regulatory demands. CISOs need to provide data-backed insights and make the business case for elevating compliance to a strategic imperative.

Executive call-to-action

As regulatory requirements continue to shape the cybersecurity landscape, it's essential that executives across the C-suite stay ahead of compliance issues while leveraging regulations as a catalyst for innovation. Creating alignment across security teams, risk functions and executive leadership is crucial for maintaining compliance readiness and driving strategic improvements.

CISOs and CROs: Deliver frequent reporting to other executive leaders on the state of regulations that directly impact respective industry or territory needs, and work towards implementing technology and regulatory change management processes.

CFOs: Verify the accuracy, completeness and defensibility of all regulatory disclosures of cyber risk management and program posture. Develop a clear understanding of materiality and the specific impact of a cyber incident, incorporating cyber risk quantification to accurately assess and communicate potential risks.

CEOs: Understand oversight responsibilities to guide compliance efforts, including any necessary coordination between different business units. Identify key questions to ask CISOs to close any knowledge gaps on compliance posture.

Chief compliance officers: Stay abreast of regulatory compliance requirements and collaborate with the CISO and CRO to incorporate proactive compliance measures and monitoring to periodically confirm compliance.

CLOs and GCs: Determine the right amount of disclosure details needed to fulfil cyber program reporting obligations, striking a balance between transparency and confidentiality.

Board: Stay abreast of emerging regulatory requirements and seek input from management on proactive measures being taken to prepare for new requirements. Understand management's approach to assessing and disclosing cyber incidents.



Unlocking the potential of cyber risk quantification: What's holding organisations back?



15%

Only 15% are measuring the financial impact of cyber risks to a significant extent

87%

say allocating resources to areas of highest risk is of high importance

44%

say data issues are a top challenge faced when quantifying the financial impact of cyber risk

As cyber threats rapidly evolve in scope and sophistication, cyber risk quantification has become a critical tool that organisations can't afford to overlook. But despite its widely acknowledged benefits, several challenges (data quality issues, output reliability, etc.) have impeded broader adoption.

Measuring cyber risk is critical but limited

While executives largely agree that measuring cyber risk is crucial for prioritising cyber risk investments (88%) and allocating resources to areas of highest risk (87%), only 15% of organisations are actually doing it to a significant extent (e.g., extensive cyber risk quantification with automation and extensive reporting).

For the organisations that do measure risk, seven in 10 executives indicate they use security posture assessments to quantify residual risk by considering the effectiveness of key controls such as compliance with vulnerability remediation, user access reviews and training completion. The adoption of more holistic cyber risk quantification practices, however, remains limited.

Benefits of quantifying cyber risk

88% To help prioritise cyber investments

88% To help evaluate and communicate cyber risks in line with defined risk tolerance

87% To help allocate resources to areas of highest risk

86% To demonstrate the cyber risk management program's value

84% To measure and compare threats and incidents on an apples-to-apples basis

Q27. Please indicate how important or unimportant the following aspects are to your organisation in quantifying cyber risk. Base: Security leaders, CEO, Board Member, CFO and CRO respondents measuring the potential financial impact of cyber risks= 1899
Source: PwC 2025 Global Digital Trust Insights

Wake-up call

It's time to realise the full potential of cyber risk quantification. The gap between recognition and implementation is a missed opportunity that can no longer be ignored. Organisations that don't measure cyber risk or haven't fully developed this capability are leaving critical intelligence on the table, particularly when it comes to informing board decisions and capital allocation.

What are the barriers to wider implementation?

Data issues, scope uncertainty and legal concerns rank high on the list of obstacles to implementing cyber risk quantification. Lack of trust in the reliability of quantification outputs is another. Further complicating adoption is the gap between what senior executives expect and what CISOs deliver, as measuring cyber risk requires alignment between security executives and business risk appetite.

Challenges faced in quantifying financial impact of cyber risk

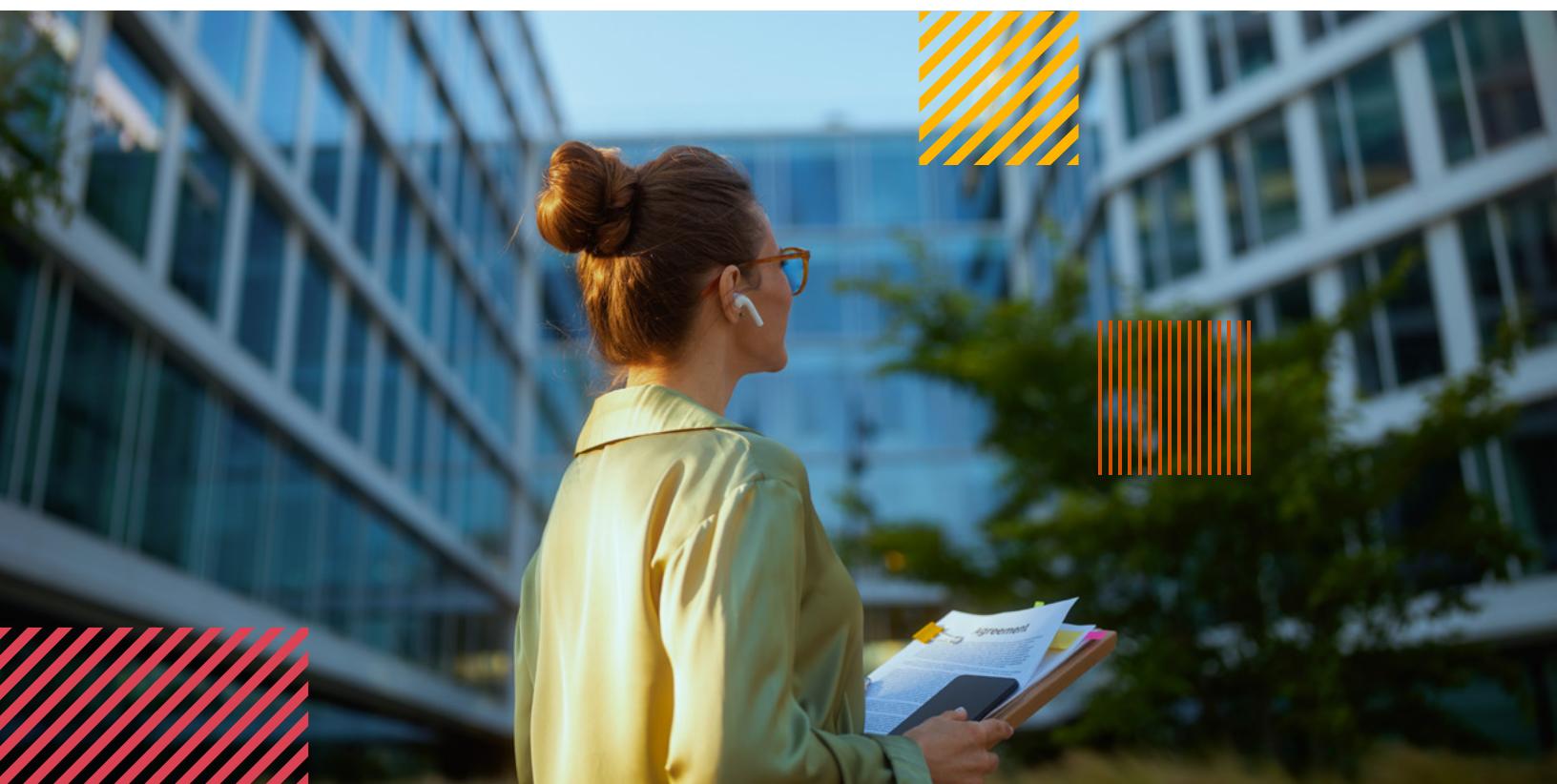
(showing % ranked 1-3)



Q26. What challenges, if any, has your organisation faced in quantifying the potential financial impact of cyber risk? (Ranked in top three) Base: Security leaders, CEO, Board Member, CFO and CRO respondents measuring the potential financial impact of cyber risks= 1899
Source: PwC 2025 Global Digital Trust Insights

Wake-up call

The barriers to cyber risk quantification adoption — and use — may be stalling progress. Organisations can't afford to let these challenges hinder critical decision-making. Address these obstacles head on, build trust in cyber risk quantification and fully integrate it into your strategic process.



Executive call-to-action

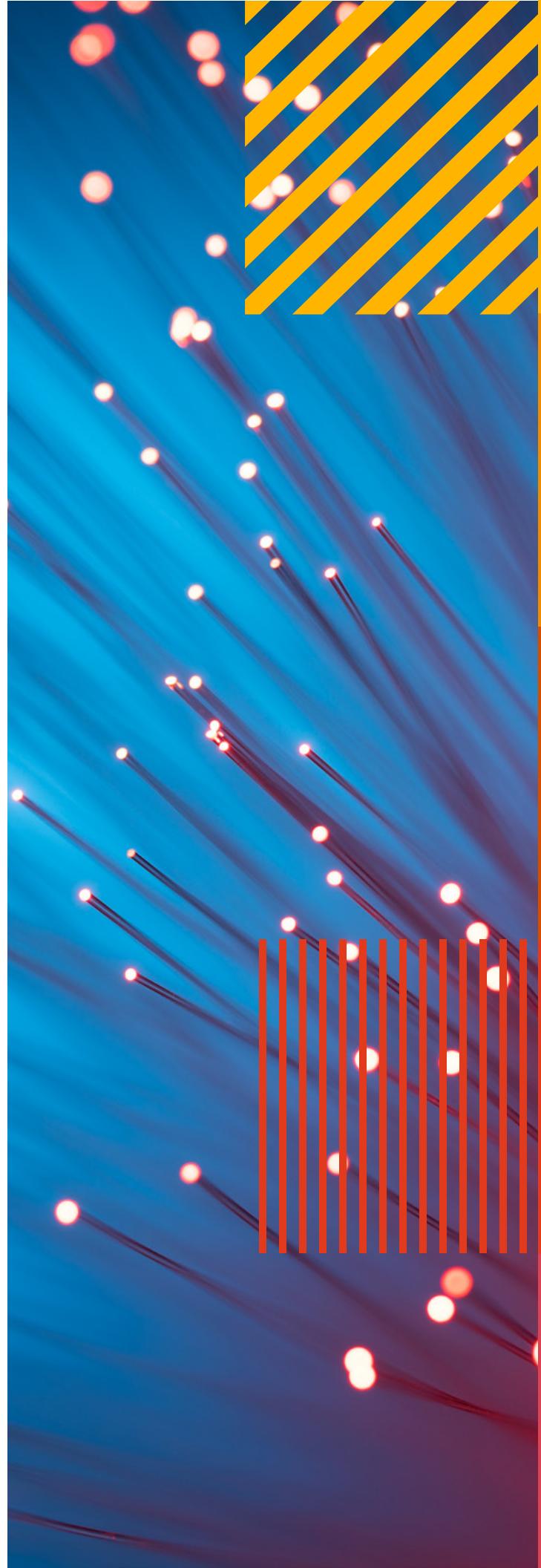
Establishing a trusted cyber risk quantification system is essential for making informed decisions and prioritising strategic investments. By accurately measuring risk, executives can align cybersecurity efforts with broader business objectives.

CISOs: Consider starting small with a specific output in mind. Leverage the information you have within your organisation (e.g., controls effectiveness, maturity, incident or loss data). New tools can help with risk quantification but aren't a requirement. Define your program and look for enabling technologies to support what you've designed.

CISOs and CROs: Show C-suite executives the most impactful financial risk measurement outcomes from quantification tools and practices. These examples can help persuade leadership to prioritise and allocate the right resources to the highest areas of risk.

CEOs: Work with your CISO and CRO to gain a deeper understanding of the business value of cyber risk quantification and the potential costs and missed opportunities from not measuring cyber risks.

Board: Understand the methods your organisation currently uses to assess cyber risk. Press management on its plans to implement risk quantification more broadly to better assess and report on the company's cyber risk posture.



Investing in resilience, building trust



77%

expect their cyber budget to increase next year

48%

of business executives prioritise data protection and data trust as the top cyber investment over the next year

34%

of tech executives prioritise cloud security as the top cyber investment over the next year

As cybersecurity continues to evolve into a critical business priority, organisations are beginning to see its potential as a key differentiator and a way to enhance their reputation and trustworthiness. To prepare, many are increasing their cyber budgets with a particular concentration on data protection and trust. By strategically investing in these areas, companies are not only building resilience but positioning themselves positively to their customers.

“ The threat landscape is increasingly unpredictable, as we’re seeing multi-vector threats to physical and digital environments. We’re investing resources toward integrated response and recovery capabilities to enhance physical security and cybersecurity. Threat actors don’t differentiate. We need to be prepared at every level with our business continuity and resilience programs.”

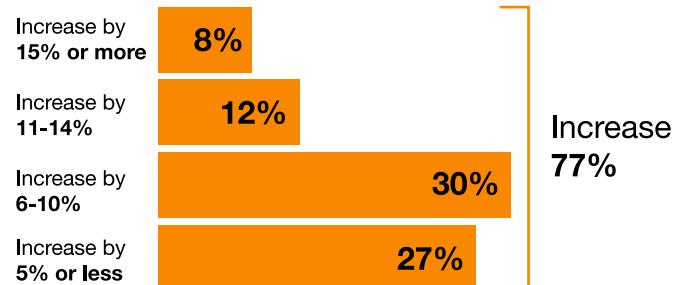
Dr. Georg Stamatelopoulos, CEO of EnBW AG

Cyber budgets are expected to grow in the next year

Cyber budgets remain in line with last year, with smaller organisations investing a higher percentage of their resources compared to larger organisations. This likely reflects smaller organisations playing catch-up in areas where larger firms have already invested heavily. Larger organisations, although expressing concerns around emerging threats and resilience, are taking a more measured approach to their investments, probably due to having more established security frameworks in place.

Over three quarters of executives expect their organisation's cyber budget to increase next year. That number is higher (82%) for organisations in North America and in the technology, media and telecom (TMT) sector.

Cyber budget change in 2025



Q7. How will your organisation's cyber budget change in 2025? Base: All respondents= 4042
Source: PwC 2025 Global Digital Trust Insights

Wake-up call

After a year of maintaining budgets, it's essential to align the planned increase in spending with both current and future risks so every dollar strengthens resilience and prepares the organisation for the evolving threat landscape.

Investing in what matters most: Cloud and data trust go hand-in-hand

Over the next 12 months, organisations are prioritising data protection/trust and cloud security above other cyber investments. They understand that securing sensitive information is vital to maintaining stakeholder trust and brand integrity.

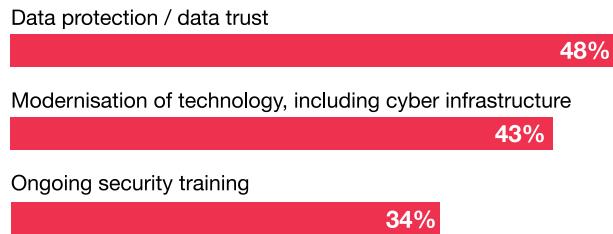
Business and tech executives rank a different list of priorities based on areas specific to their roles.

Business executives say data protection/trust is their top cyber investment priority (**48%**), followed by tech modernisation and optimisation (**43%**).

For tech executives, cloud security remains their top priority (**34%**), following the same trend from last year. Data protection and trust is the next priority (**28%**).

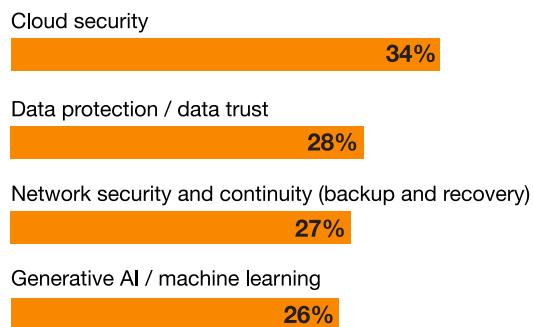
Cyber investment priorities for business leaders

(showing % ranked 1-3)



Cyber investment priorities for tech leaders

(showing % ranked 1-3)



Q8a. Which of the following investments, if any, are you prioritising when allocating your organisation's cyber budget in the next 12 months? (Ranked in top three) Base: All Business respondents with awareness of cyber budget change= 1867
Source: PwC 2025 Global Digital Trust Insights

Q8b. Which of the following investments, if any, are you prioritising when allocating your organisation's cyber budget in the next 12 months? (Ranked in top three) Base: All Tech respondents with awareness of cyber budget change= 2092
Source: PwC 2025 Global Digital Trust Insights

Why does cloud security continue to demand attention? Despite years of investment, the rapid adoption of cloud technologies, the consolidation of cloud hyperscalers and the rise of hybrid and multi-cloud setups have concentrated risk in the cloud environment. This concentration heightens the potential impact of data access misconfigurations, data breaches and integration challenges. As threat actors evolve, so must cloud security strategies, making continued investment crucial for mitigating these intensified risks.

Wake-up call

Investing in cybersecurity is investing in trust. Whether it's securing the cloud, safeguarding data or addressing emerging risks, your commitment to these areas will shape stakeholder confidence and your organisation's resilience.

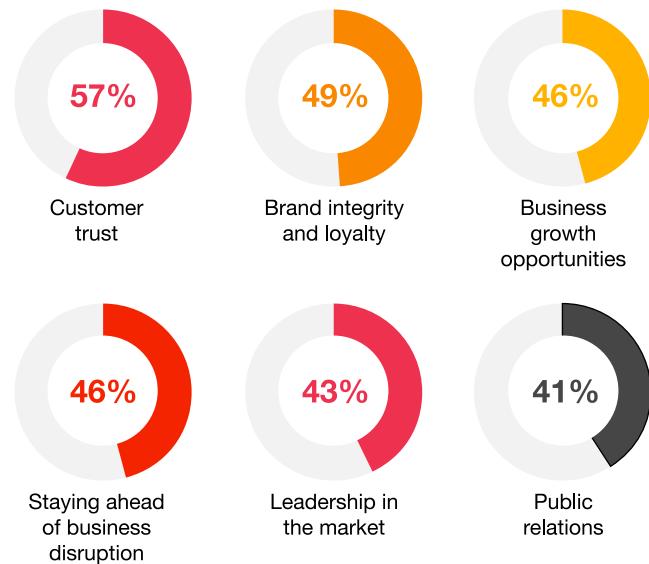


Cybersecurity and trust: The new competitive edge

Organisations increasingly view cybersecurity as a key differentiator for a competitive advantage, with 57% of executives citing customer trust and 49% citing brand integrity and loyalty as areas of influence. As cyber threats escalate, a strong cybersecurity posture isn't just about protection — it's about building a reputation that customers and stakeholders can rely on. At a time when [trust is paramount](#), companies that prioritise cybersecurity are better positioned to stand out as leaders in both safety and integrity.

Positioning cybersecurity as a competitive advantage

(showing % selected 'To a large extent')



Q19. To what extent does your organisation position cybersecurity as a competitive advantage in these areas? Base: All respondents= 4042
Source: PwC 2025 Global Digital Trust Insights

Wake-up call

Your cybersecurity isn't just safeguarding data, it's safeguarding your brand. In a competitive landscape, trust is everything. Strengthen your security measures now to help your organisation stand out as a leader in data integrity.

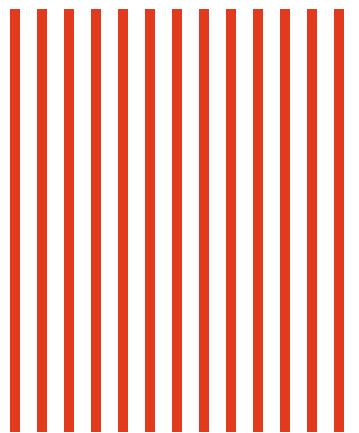
Executive call-to-action

With cybersecurity investments poised to grow, it's essential for every member of the C-suite to align their strategies with the organisation's most pressing risks. Executives should make investments that not only address current vulnerabilities but also build trust and resilience.

CIOs, CTOs and CISOs: Translate the business case for data protection and cloud security investment priorities to CFOs based on the business value of key outcomes (e.g., reducing the time to recover mission-critical data or patching a system).

CFOs: Determine the business value of data protection and cloud security to gain stakeholder trust and make more informed cybersecurity investment decisions.

CDOs: Collaborate with tech, security and finance executives to pinpoint the most essential data security and integrity priorities to guide the information and cloud security investment strategy. Confirming data quality and readiness is necessary to increase security investments.



Is your cyber strategy and leadership driving real resilience?



2%

Only 2% have implemented cyber resilience actions across their organisation in all areas surveyed

21%

Only 21% usually allocate cyber budget to the top risks of the organisation

50%

Under 50% of CISOs are involved to a large extent in strategic planning on cyber investments

To manage tomorrow's threats, investments alone are not sufficient — organisations should also elevate their approach to cyber strategy and leadership. From lagging resilience efforts to gaps in CISO involvement in strategic decisions, there are clear areas where strategic alignment is needed. To get there, organisations should emulate the leading cybersecurity practices of their top performing peers. They should also move beyond addressing known threats and implement an agile, secure-by-design approach to business, one that strives to build trust and lasting resilience.

“ It’s the CISO’s job to contextualise and connect the threats that exist to the vulnerabilities within the organisation. That means educating people on the threats the enterprise is prepared to deal with and those it’s not ready for. With an education-forward approach, there tends to be more cooperation across the organisation.”

David Bruyea, CISO at Moneris

Partial implementation isn't enough

Despite mounting concern about cyber risk, most businesses are struggling to fully implement cyber resilience across core practices. A review of 12 resilience actions across people, processes and technology indicates that 42% or fewer of executives believe their organisations have fully implemented any one of those actions. More concerning, only 2% say all 12 resilience actions have been implemented across their organisation. This leaves a glaring vulnerability — without enterprise-wide resilience, companies remain dangerously exposed to the increasing threats that could compromise the entire operation.

Here are just a few key areas that would benefit from cross-organisational attention.

Establishing a resilience team (only 34% of executives say this has been implemented across the organisation)

Developing a cyber recovery playbook for IT-loss scenarios (only 35% say this has been implemented across the organisation)

Mapping technology dependencies (only 31% say this has been implemented across the organisation)

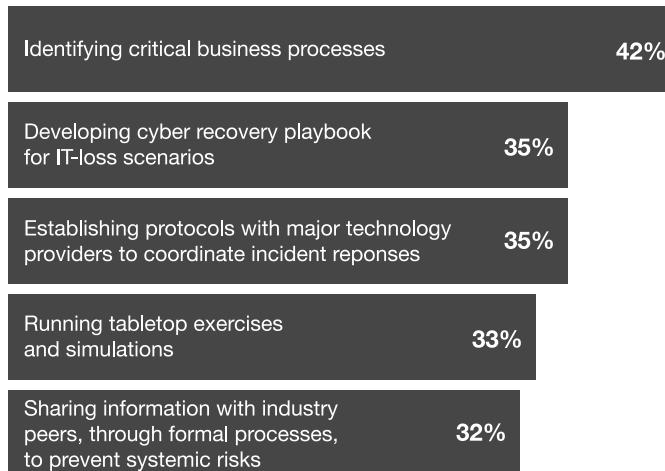


Implementation of cyber resilience actions across the organisation

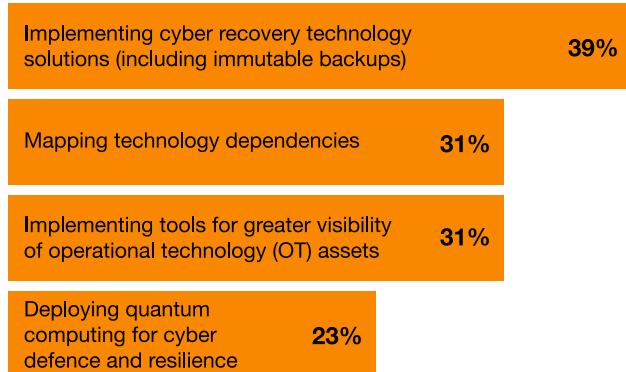
People



Processes



Technology



Q10. To what extent is your organisation implementing or planning to implement the following cyber resilience actions? Base: All respondents= 4042
Source: PwC 2025 Global Digital Trust Insights

Wake-up call

Lagging cyber resilience puts your organisation at risk. Take enterprise-wide action through technology, processes and people to transform your defences and prepare for the challenges ahead.

Cyber resilience is a key priority. Why are so many companies behind in critical areas?

Many companies still lag when it comes to demonstrating leading cybersecurity practices. Only around one in five executives note they demonstrate these practices on a usual basis. Just 20%, for instance, usually anticipate future cyber risks and only 21% usually allocate cyber budget to the top risks of the organisation. This lag could be due to several factors, including a lack of strategic foresight, insufficient resources or a reactive rather than proactive approach to cybersecurity.

Behaviours an organisation's cybersecurity team 'usually' performs

(81-100% of the time)

Puts controls in place and responds quickly to threats so our organisation can withstand serious cyber disruptions



Collaborates with other parts of the business that affect the organisation's cybersecurity posture



Delivers insights on changing cyber risk exposure, regulatory developments and mitigation measures to the CEO and board



Allocates cyber budget to the top risks of the organisation



Anticipates future cyber risks given the macro environment, emerging technology and business strategy



Q28. Finally, please indicate how consistently your organisation's cybersecurity team does the following. Base: All respondents= 4042
Source: PwC 2025 Global Digital Trust Insights

Top performers consistently and significantly outshine the rest

We explored this question further to identify a group of top performing executives who “usually” demonstrate these behaviours. There’s a gap of 69 percentage points greater across all behaviours between top performers and our overall global respondents. Top performers are more likely to have higher confidence in their organisation’s ability to comply with regulations and have implemented key resilience actions across their organisation.

Difference in behaviours of cybersecurity teams between top performers and all leaders

% responding ‘Usually (81-100% of the time)’

Anticipates future cyber risks given the macro environment, emerging technology and business strategy



Collaborates with other parts of the business that affect the organisation’s cybersecurity posture



Allocates cyber budget to the top risks of the organisation



Puts controls in place and responds quickly to threats so our organisation can withstand serious cyber disruptions



Delivers insights on changing cyber risk exposure, regulatory developments and mitigation measures to the CEO and board



All respondents

Top performers

Q28. Finally, please indicate how consistently your organisation’s cybersecurity team does the following. Base: All respondents= 4042, Top performers = 222
Source: PwC 2025 Global Digital Trust Insights

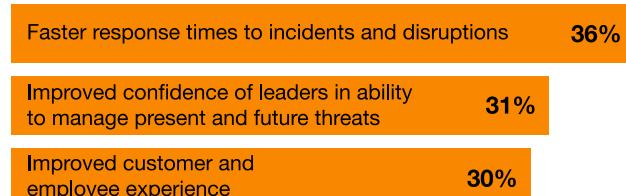
Wake-up call

To close the gap, organisations need to shift from reactive to proactive cybersecurity strategies. This includes better risk anticipation, more strategic budget allocation and a commitment to continuous improvement.

Strategic priorities: Speed, trust and stakeholder security

Over the next 12 months, more than a third of executives expect to work on reducing response times to incidents and disruptions. Other top goals include boosting confidence in leadership’s ability to manage threats and enhancing the experiences of both customers and employees. These goals reflect a broader push to not only mitigate risks faster but also build trust and safeguard customers and employees.

Organisation’s goals relating to cyber and privacy (showing % ranked 1-3)



Q23. What, if any, are your organisation’s strategy, people and investment goals relating to cyber and privacy over the next 12 months? (Ranked in top three)
Base: All respondents= 4042
Source: PwC 2025 Global Digital Trust Insights

Wake-up call

Quick responses aren’t just a goal — they’re a necessity. Delayed reactions to threats can cost more than just time. They can erode trust and severely disrupt your business. Speed and confidence in leadership should be nonnegotiable priorities.

Elevating the CISO: Aligning strategy with security

Many organisations miss critical opportunities by not fully involving their CISOs in key initiatives. Fewer than half of executives tell us that their CISOs are largely involved in strategic planning for cyber investments, board reporting and overseeing tech deployments. This gap leaves organisations vulnerable to misaligned strategies and weaker security postures.

CISO involvement in business activities 'to a large extent'



Q21. How involved is your organisation's CISO in taking an active role in the following areas? Base: All respondents except CISO= 3640
Source: PwC 2025 Global Digital Trust Insights

Executive call-to-action

Strong cybersecurity leadership demands strategic vision and alignment across the organisation. Each executive has a role in driving this alignment, from integrating the CISO into key decisions to prioritising resilience efforts.

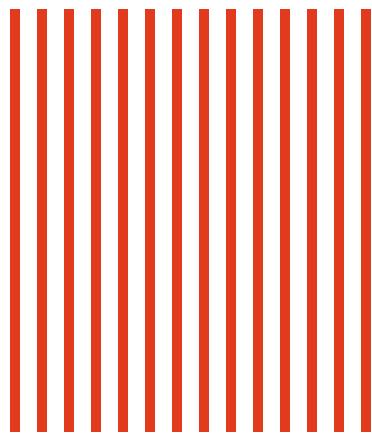
CISOs: Make the business case to the rest of the C-suite for why it's imperative that CISOs be involved in strategy, planning and oversight of the cyber risk mitigation and resilience strategy.

CEOs, CFOs and CIOs: Participate in cyber resilience assessments and exercises to better understand gaps and approaches CISOs might face for integrating leading practices, standards and controls.

Board: Stay informed on cyber risk program developments, especially related to your organisation's cyber risk and threat exposure, to meet expanding oversight and governance responsibilities.

Wake-up call

Give your CISO a seat at the table. Their insights are vital for proactively navigating cybersecurity as a core business enterprise risk. Involving them at the highest level helps your organisation align its approach to safeguarding critical assets and driving resilience.





About this report

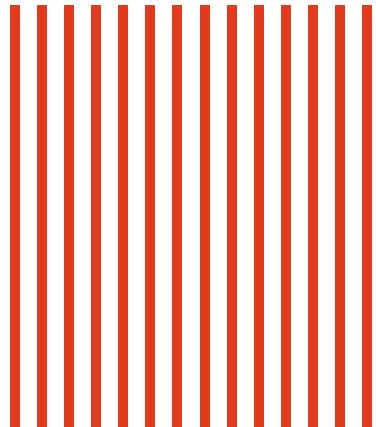
The 2025 Global Digital Trust Insights is a survey of 4,042 business and technology executives conducted in the May through July 2024 period.

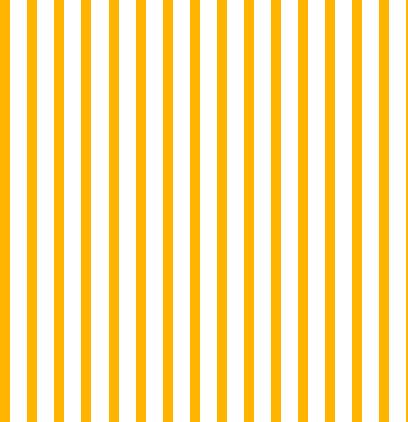
A quarter of the executives are from large companies with \$5 billion or more in revenues. Respondents operate in a range of industries, including industrials and services (21%); tech, media, telecom (20%); financial services (19%); retail and consumer markets (17%); energy, utilities and resources (11%); health (7%) and government and public services (4%).

Respondents are based in 77 countries. The regional breakdown is Western Europe (30%), North America (25%), Asia Pacific (18%), Latin America (12%), Central and Eastern Europe (6%), Africa (5%) 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 27th 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

Global Cybersecurity & Privacy Leader
US Cyber, Risk & Regulatory Leader
PwC US

sean.joyce@pwc.com | [LinkedIn](#)

