pwc

The C-suite playbook:

Putting security at the epicenter of innovation

Findings from the 2024 Global Digital Trust Insights

Security at the epicenter of innovation: That's not the world we live in today, but what if it were?

While excitement and budgets are rising for cutting-edge security programmes, progress on actually improving security is sluggish, even stagnant.

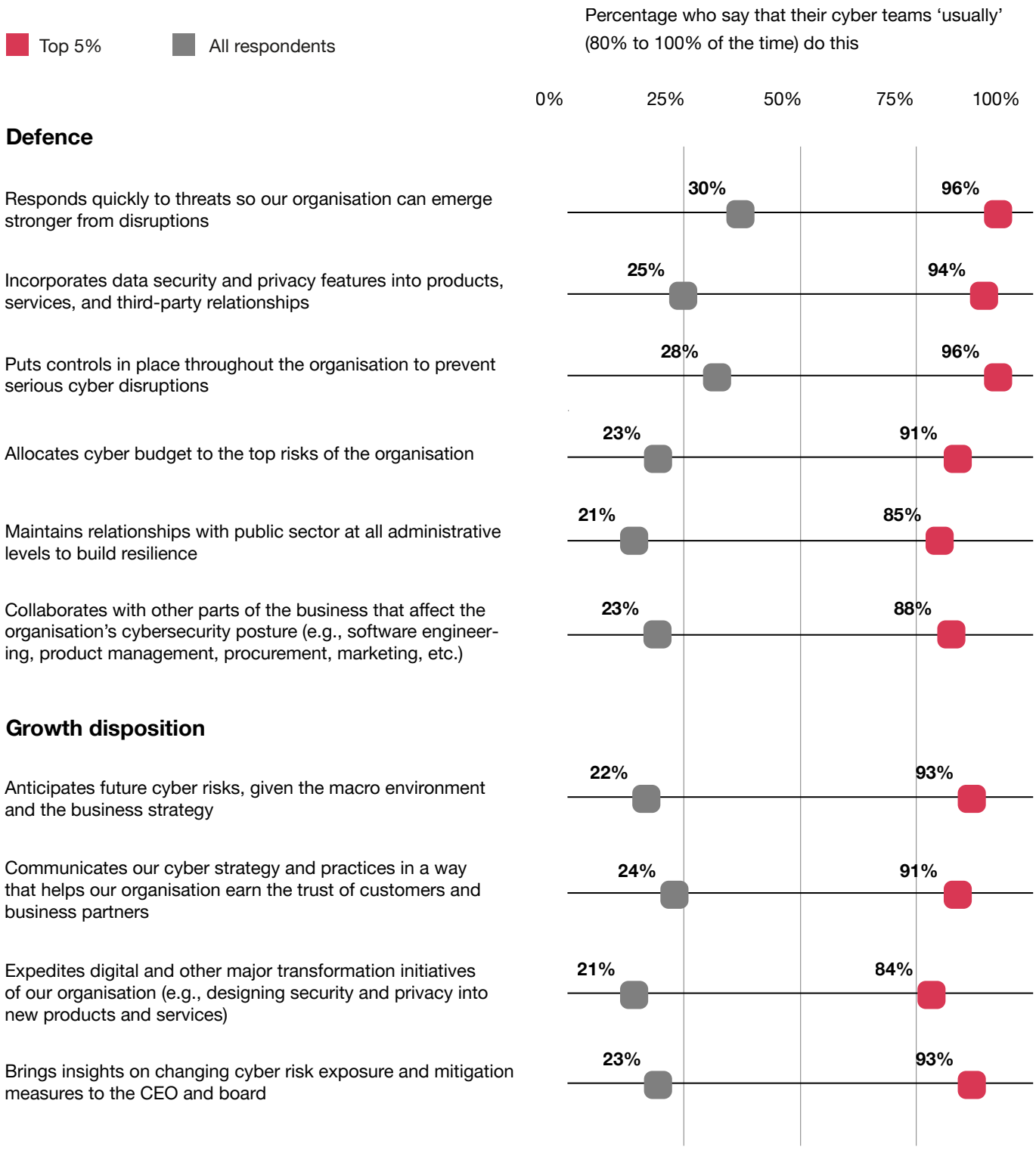
PwC's 2024 Global Digital Trust Insights survey of 3,876 business and tech executives at the largest global companies — 30% of respondents have revenues of $10 billion or more — shows considerable room for improvement in cybersecurity.

Consider these findings. Breach costs and the number of high-dollar breaches continue to increase. Although cloud attacks are the top cyber concern, about one-third of organisations have no risk management plan to address cloud service provider challenges. Only half are 'very satisfied' with their technology capabilities in key cybersecurity areas. More than 30% of companies don't consistently follow what should be standard practices of cyber defence.

Imagine a world with security at the epicenter of innovation — the field where bright ideas and bold ambitions flourish. Imagine the CISO right there, working to secure the organisation's lofty ambitions and prized assets.

We note 179 respondents who seem to be doing just that. These top 5% — our stewards of digital trust — are reaping benefits that others are missing. They're experiencing fewer breaches, and the attacks that do hit them aren't as costly. Managing risk is easier because they've streamlined their security solutions. And they've positioned themselves for greater productivity and faster growth, outpacing the competition as they plunge into new technologies with confidence that they are well protected.

Meet our stewards of digital trust



Q26. Please indicate how consistently your organisation's cybersecurity team does the following.
Base: All respondents= 3876
Source: PwC, 2024 Global Digital Trust Insights.

With technology now at the heart of business, safeguarding it is tantamount to protecting the enterprise. That's why in 2023, PwC created a playbook for C-level executives to help each C-level executive focus on the questions they need to answer with their CISO.

We've updated the playbook for 2024. This is likely to be a watershed year. Cybersecurity faces four major shifts, each of which could be disruptive on its own.

- C-suite insistence on modernising and improving technology infrastructure and investments in a year of cost-cutting and macroeconomic uncertainty.
- The rise of hybrid cyber threats and the blurring of the line between espionage and cybercrime, propelling cyber defence more fully into the national security arena.
- A groundbreaking new technology — generative AI — bringing new threats as well as unprecedented promise for defence.
- Regulations requiring openness about cyber incidents and risk management practices that could usher in a new era of transparency and collaboration.

Businesses are reinventing themselves. Policymakers are thinking of new regulatory approaches. Are your senior executives being similarly innovative in the way they secure their organisations? How bold can you be, and what might you do differently?

9 degrees of separation: Top performers vs the rest

Top 5% are:

6x more likely to have already implemented transformative cybersecurity initiatives from which they are realising benefits.

5x more likely to be very satisfied with their current cyber technology capabilities.

4x more likely to be continually updating their risk management plan to mitigate cloud risks.

9x more likely to be mature in their cyber resilience practices.

Source: PwC, 2024 Global Digital Trust Insights.

Top 5% are more likely to:

Invest more into cyber budget, with **85% increasing their cyber budget in 2024** (vs 79% overall), of which 19% are increasing cyber budget in 2024 by 15% or more, compared to 10% overall.

Say their **most damaging cyber breach** in the last three years cost them less than $100k (28% vs 19% overall).

Strongly agree their **organisation will develop new lines of business using generative AI (GenAI)** (49% vs 33% overall).

Plan to deloy GenAI tools for cyber defence (44% vs 27%).

Disagree that 'GenAI will lead to a catastrophic cyber attack' (33% vs 22% overall).

Cyber risk management: Ripe for reinvention

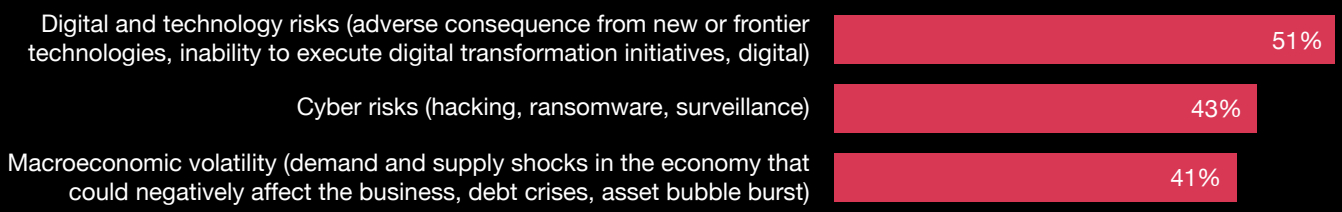
Innovation means making bold moves, and there's nothing more empowering than knowing that you've done what's possible to remain safe and secure — that you've assessed and addressed your most important cyber risks.

Mitigating cyber risk is a top priority for 2024, according to PwC's 2024 Global Digital Trust Insights survey. After dropping to fourth place in last year's PwC CEO Survey, it's now second for our respondents, behind only digital and technology risks on the list of prioritized risks. And in the minds of our respondents, digital and technology risks are inextricable from cyber risk.

In today's business climate, we simply can't talk about digital transformation or reinvention without mentioning cybersecurity in the same breath. Cloud attacks and attacks on connected devices are the cyber threats our respondents are most concerned about — two technologies at the heart of business transformation today.

Digital tops the risk list in two ways

Risk mitigation priorities over the next 12 months (Ranked top three)



Q1. Which of the following risks is your organisation prioritising for mitigation over the next 12 months? (Ranked in top three).
Base: All respondents= 3876
Source: PwC, 2024 Global Digital Trust Insights.

These cyber threats themselves are connected. Once malicious actors break into systems and networks, they often wreak havoc in as many ways as possible.

What may start as a cloud breach could very well become an advanced persistent threat as bad actors lurk inside your system collecting data and looking for other ways to do harm. They might exfiltrate your data, then launch a ransomware attack, then leak the data ("hack and leak") even if you pay the ransom.

Any one of these incidents would be problematic on its own. Taken all together, they can devastate your business operations and your reputation. Mega breaches are increasing in number and scale — and cost. The percentage of those reporting costs of $1 million or more for their worst breach in the past three years rose to 36% from 27% last year.

The pace of business reinvention and innovation using technology is not slowing down. Not when 40% of CEOs think their companies may no longer be economically viable a decade from now if they stay on their current path. The C-suite challenge is this: Is your organisation's cyber risk management keeping up with the changes?

The C-suite challenge is this: Is your organisation's cyber risk management keeping up with the changes?

Everything is connected, including cyber attacks

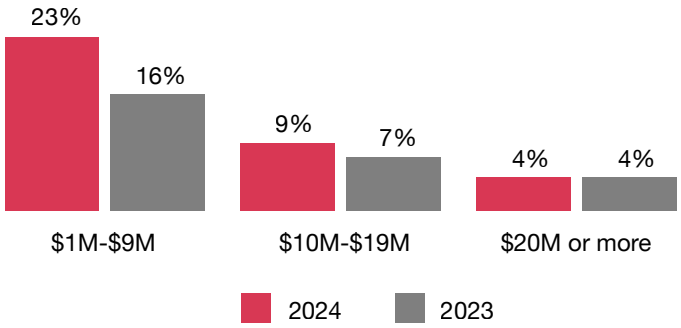
Top cyber threats over the next 12 months

Q3. Over the next 12 months, which of the following cyber threats is your organisation most concerned about? (Ranked in top three).
Base: All respondents=3876
Source: PwC, 2024 Global Digital Trust Insights.

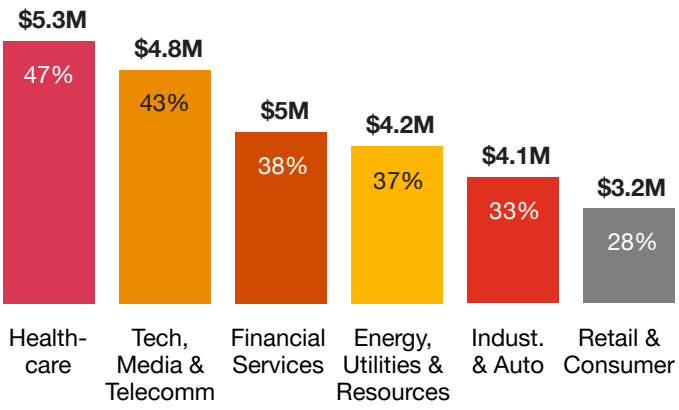
Breaches are becoming more costly

Estimated costs to organisations' most damaging data breach in the past three years

Percentage who say they had a $1M+ breach:
2024 total = 36%, 2023 total = 27%



Average cost of breach in millions and percentage of most damaging breaches that cost $1 million or more, by sector



Q5. Thinking about the most damaging data breach you experienced in the past three years, please provide an estimate of the cost to your organisation. Base: Security and IT and CFO respondents= 1651
Source: PwC, 2024 Global Digital Trust Insights.

Simplification of cyber tools: The bane of bad actors

Modernisation and optimisation top the cyber-investment priorities for 2024. Nearly half (49%) of the business leaders selected technology modernisation, including cyber infrastructure, and 45% chose optimisation of existing technologies and investments.

In our 2022 survey we found that CEOs in particular were very concerned that their organisations had become too complex to secure. At that time, 32% had consolidated technology vendors in an effort to simplify, as well as realign their mix of managed and in-house services.

In the 2024 survey, 44% report using an integrated suite of cyber tech solutions, and 39% plan to move to one in the next two years. Nearly one-fifth — 19% — say they have too many cyber solutions and need to consolidate.

An overabundance of point solutions may be one reason why only 5% of IT and tech respondents say they're 'very satisfied' with the technology capabilities of their cyber solutions in all eight key areas. Software that doesn't work together can hinder performance, require more time to manage and impede the big-picture view that's essential to managing cyber risk.

Those who've already been hit know this. Our survey respondents who have had data breaches costing $1 million or more in the past three years are more likely to acknowledge that they have too many cybersecurity solutions and need to integrate them. On the other hand, organisations that use cohesive cyber-solution suites are more often able to avoid the big, costly breaches.

2024 cyber budgets aim to make the most of existing tools

Business leaders - Cybersecurity investment priorities over the next 12 months (Ranked top three)

Q14b. Which of the following investments are you prioritising when allocating your organisation's cyber budget in the next 12 months? (Ranked in top three). Base: Business respondents= 1925
Source: PwC, 2024 Global Digital Trust Insights.

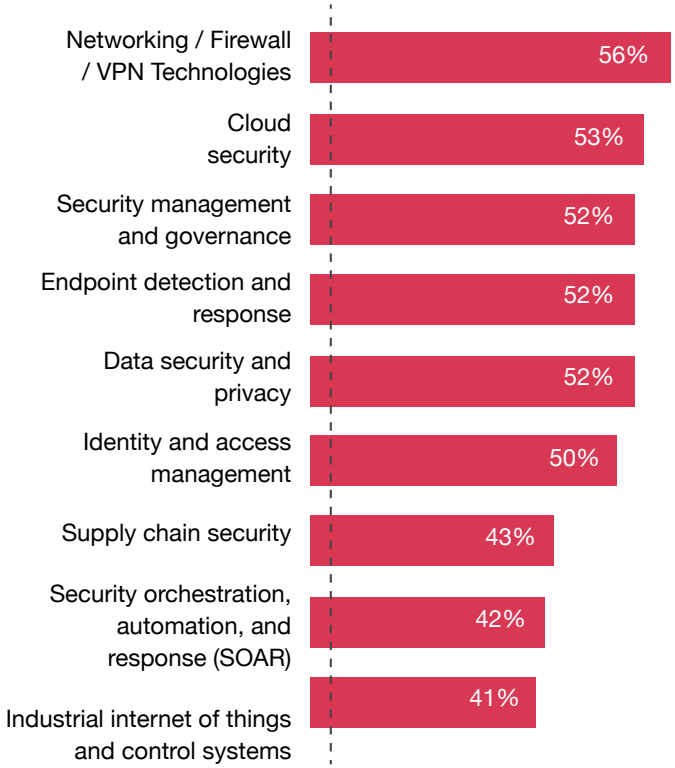
Still, survey respondents aren't pulling in the reins on spending. More than three-quarters (79%) say they'll increase their cyber expenditures in 2024 (up from 64% last year), especially large organisations with revenues of $5 billion or more. Those planning larger budget increases of more than 15% tend to be enterprises with $50 billion or more in revenues, or in tech, media and telecom industries, or those that project higher revenue growth in the next year.

Cyber investments are also making up a larger proportion of the total IT, OT and automation budget. We're seeing a mean increase overall to 14% in 2024 versus 11% for 2023.

The C-suite challenge isn't a lack of tools or a lack of investment. Instead, it's figuring out how your organisation can reap the benefits of your investments. Is your IT architecture too complex to adequately protect? Are you making it easy for threat actors to find gaps in your defence?

Only half are satisfied with their cyber-tech capabilities

Organisation's technology capabilities in key cybersecurity areas



Only 5% of security and IT respondents are very satisfied across all areas

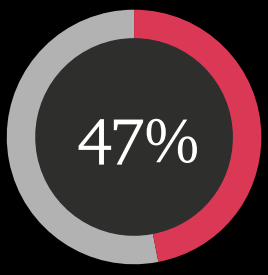
Q23. How satisfied are you with your organisation's technology capabilities in the following areas? Base: Security and IT respondents= 1517
Source: PwC, 2024 Global Digital Trust Insights.

Cloud security: Overdue for concerted attention

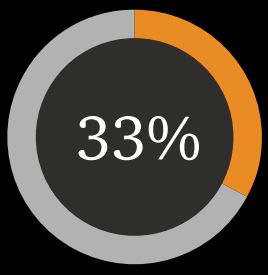
Cloud use has always been about business innovation — enabling developers to collaborate no matter where in the world they might be; adopting new, more flexible ways to work; inventing new business models; connecting technologies to help better operate the business; providing superior service to customers and clients; and so on.

Cloud security is the No. 1 cyber risk concern for nearly half (47%) of our respondents. The ways bad actors might get in may seem virtually limitless. Organisations should place controls everywhere: on identity and access, lateral movement, email accounts, website portals, applications, proprietary information, customer interactions, operating systems, connected devices, the list goes on.

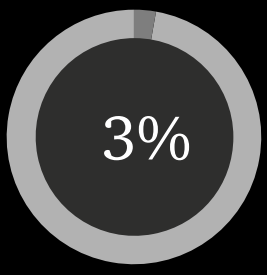
Cloud security: top threat, top investment — yet poorly managed



Top threat



Top cyber investment



Implemented and continually updating risk management plan

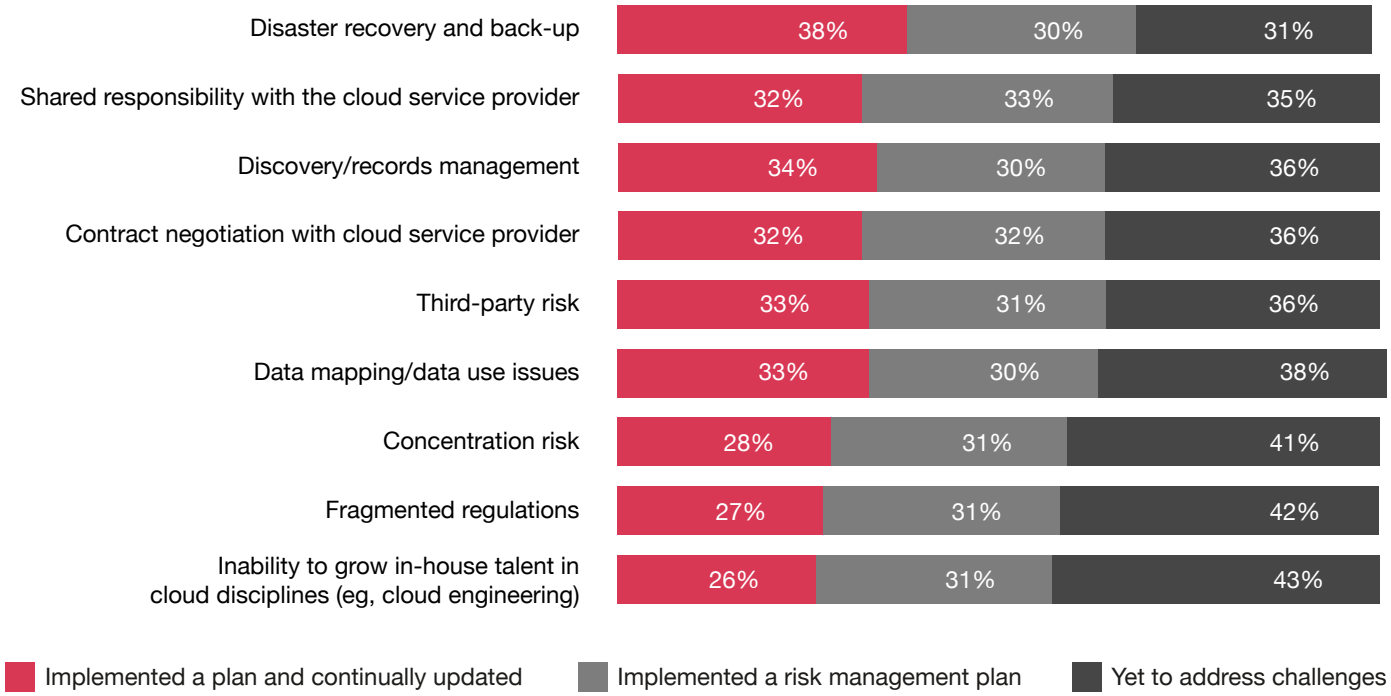
Q3. Over the next 12 months, which of the following cyber threats is your organisation most concerned about? (Ranked in top three)
Base: All respondents= 3876
Q14a. Which of the following investments are you prioritising when allocating your organisation's cyber budget in the next 12 months? (Ranked in top three) Base: IT respondents= 1919
Q19. To what extent has your organisation addressed the following challenges with your cloud service provider(s)? Base: Cloud provider users= 3648
Source: PwC, 2024 Global Digital Trust Insights.

Many of our respondents — 42% — use more than one cloud, and concerns over cloud security increase among users of multiple — hybrid — clouds. Fifty-four percent of these respondents cite cloud as their most pressing cybersecurity risk. Hybrid cloud users are also the most likely to select cloud among their top three priorities for security investments over the next year (36% as opposed to 33% overall).

But nearly every organisation — 97% — has gaps in its cloud risk management plan. Only 3% maintain up-to-date plans that address all nine cloud security areas. Risks posed by fragmented regulations, for instance, have yet to be addressed by 42%; 41% have no plan for dealing with concentration risk; 36% haven't yet addressed third-party cloud risk.

So many cloud risks, so few plans to manage them

Organisation's position on cloud service provider challenges



Q19. To what extent has your organisation addressed the following challenges with your cloud service provider(s)?
Base: Cloud provider users= 3648
Source: PwC, 2024 Global Digital Trust Insights.

The top 5% — our "stewards of digital trust" — are four times more likely to be continually updating their risk management plan to mitigate cloud risks. The remainder of our respondents, however, have yet to do so much of this critical work.

The C-suite challenge is this: How do you work together and with your cloud security providers to make headway in defending the most important entry points to your systems and assets via the cloud?

Generative AI for cyber defence on the rise

Nearly seven in 10 say their organisation will use generative AI (GenAI) for cyber defence. GenAI tools can help reduce a disadvantage for cyber teams overwhelmed by the sheer number and complexity of human-led cyber attacks, both of which continually increase.

GenAI for cyber defence

69%

More than two-thirds (69%) say they'll use GenAI for cyber defence in the next 12 months.

47%

Nearly half (47%) are already using it for cyber risk detection and mitigation.

21%

One-fifth (21%) are already seeing benefits to their cyber programmes because of GenAI – mere months after its public debut.

Q7. To what extent do you agree or disagree with the following statements about Generative AI?
Q10. To what extent is your organisation implementing or planning to implement the following cybersecurity initiatives?
Base: All respondents= 3876
Source: PwC, 2024 Global Digital Trust Insights.

Platforms are licensing their large language models (LLMs) in tandem with their cyber tech solutions. Microsoft Security Copilot intends to provide GenAI features for security posture management, incident response and security reporting. Google announced Security AI Workbench for similar use cases.

Many vendors are pushing the limits of GenAI, testing what's possible. It could be some time before we see broad-scale use of defenceGPTs. In the meantime, here are the three most promising areas for using GenAI in cyber defence.

- **Threat detection and analysis.** GenAI can be invaluable for proactively detecting vulnerability exploits, rapidly assessing their extent — what's at risk, what's already compromised and what the damages are, and then presenting tried-and-true options for defence and remediation. GenAI can help identify patterns, anomalies and indicators of compromise that elude traditional signature-based detection systems.
- **Cyber risk and incident reporting.** GenAI might also make cyber risk and incident reporting much simpler. With the help of natural language processing (NLP), GenAI can turn technical data into concise content that nontechnical people can understand. It can help with incident response reporting, threat intelligence, risk assessments, audits and regulatory compliance. And it can present its recommendations in terms that anyone can understand, even translating confounding graphs into simple text.
- **Adaptive controls.** Securing the cloud and software supply chain requires constant updates in security policies and controls — a daunting task today. Machine learning algorithms and GenAI tools could soon recommend, validate and draft security policies and automate controls that are tailored to an organisation's threat profile, technologies and business objectives.

The C-suite challenge is this: How do you wield the new tools without inviting new risks to flare up in the organisation and in society? What should you do to use GenAI ethically and responsibly?

Regulations: Providing a safe place to play and grow

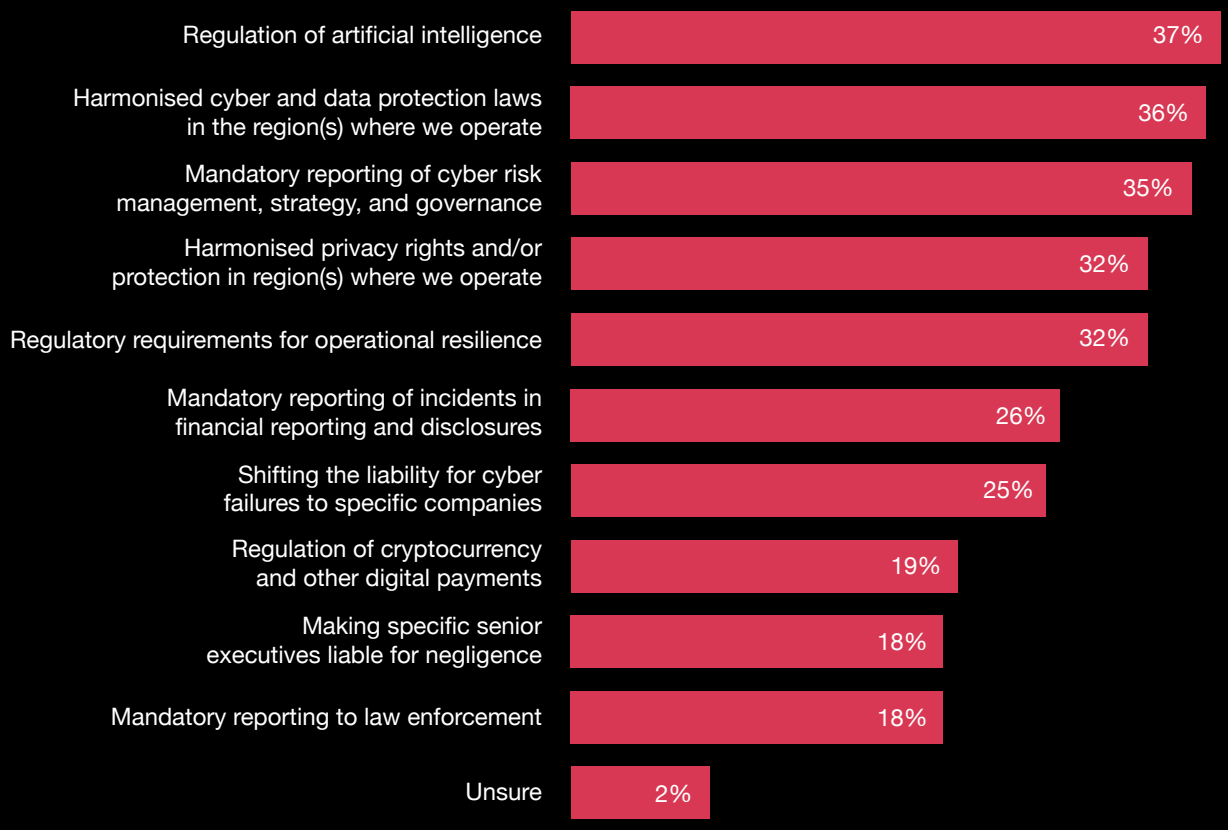
The mainstream view is that new rules and regulations hinder revenues, but here's the take of at least one-third of respondents: The guardrails regulators put up can give companies added confidence to explore, experiment, invent and compete. Navigating regulatory requirements can become a competitive advantage for leading companies.

About a third of this year's respondents agree that four types of regulation will be most important to securing the future growth of their organisation — regulation of AI (37%), harmonisation of cyber and data protection laws (36%), mandatory reporting of cyber risk management, strategy and governance (35%) and operational resilience requirements (32%).

Transparency is the regulatory drumbeat that will grow louder around the world. New SEC rules require public disclosure of cybersecurity breaches deemed to have a potential material effect on investors. The Digital Markets Act and the Digital Services Act require transparency in data practices and algorithmic decision-making. And regulations are on the horizon governing AI — including an EU AI Act in the works and GenAI regulation.

Regulations that could change cybersecurity

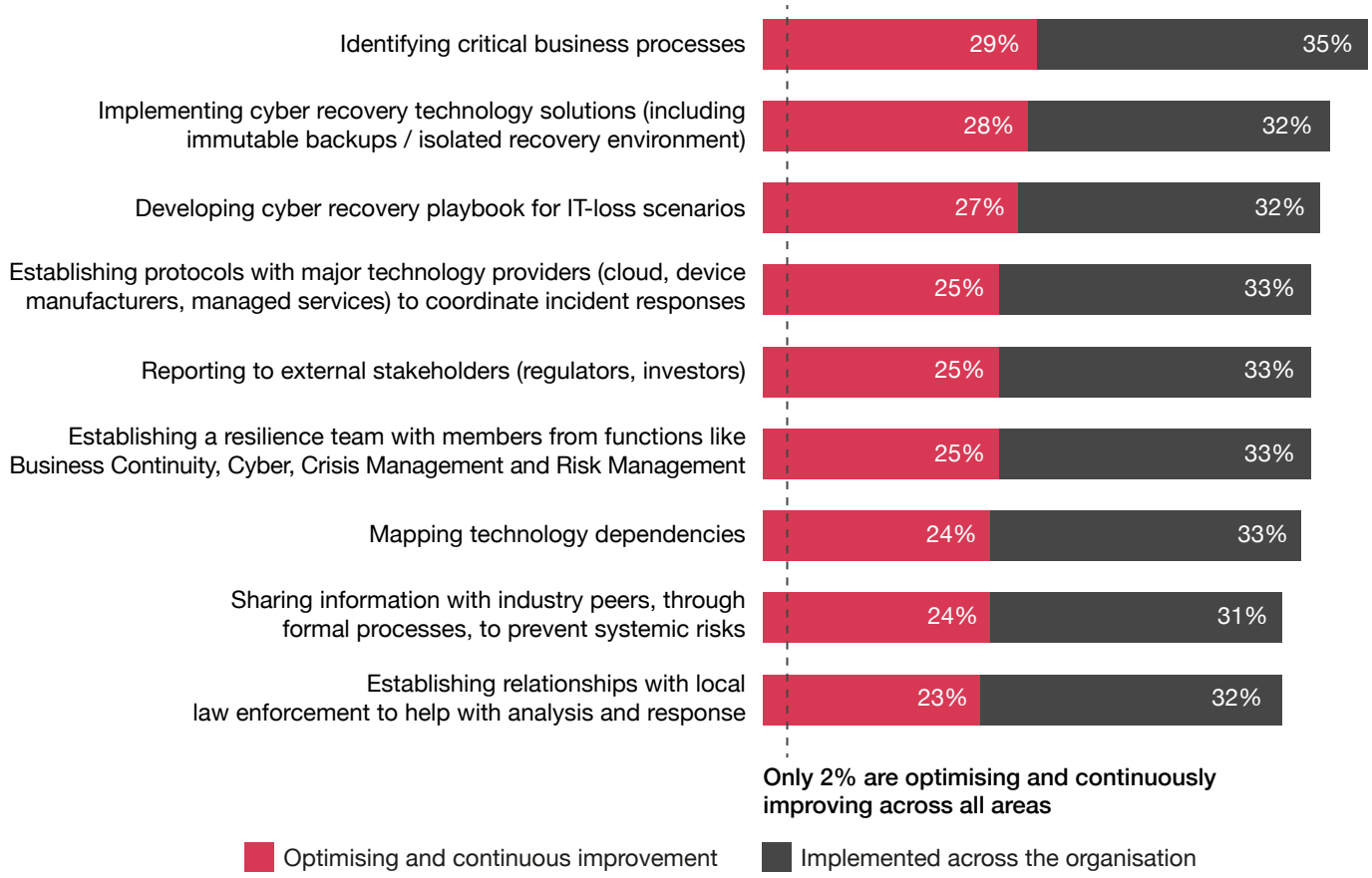
Regulatory goals and principles with the greatest impact to organisation's future revenue growth (Ranked top three)



Q24. Which of the following proposed regulatory goals and principles will have the greatest impact on your organisation's ability to secure future revenue growth? (Ranked in top three). Base: All respondents= 3876
Source: PwC, 2024 Global Digital Trust Insights.

The slow progress on cyber resilience

Extent of implementation for key cybersecurity resilience actions



Q8. To what extent is your organisation implementing or planning to implement the following cyber resilience actions?
Base: All respondents= 3876
Source: PwC, 2024 Global Digital Trust Insights.

Operational resilience is another important theme. Regulators know that it's a big risk to approach the challenge of interrelated and complex risks as many C-suite teams still habitually do — as a silo-based exercise that treats each business unit's risk profile as separate. New requirements such as the Digital Operational Resilience Act will increasingly insist on integrated resilience with core elements that make an organisation adaptive, flexible and stronger after every disruptive event.

As many as three-quarters expect that compliance with these regulations will require significant outlays of money and time. Incurring high costs and revenue impacts may be avoidable, if businesses involve themselves early and often in regulatory processes — meeting with law enforcement, for example, participating in public comments and even taking a seat at the table with regulators to help craft or influence proposed directives.

The C-suite challenge is this: Amid regulatory uncertainty, can you give your organisation the room to innovate while keeping security and privacy by design? How do you turn this new regulatory environment as a source of competitive advantage?

Dare to break cyber-as-usual: The 2024 C-suite playbook

It's no longer business-as-usual at your organisation. But most companies are still locked into cyber-as-usual, as the 2024 Global Digital Trust Insights survey shows. Fragmented initiatives. An ever-expanding array of technological complexities. A risk management programme that, with its gaps, is risky in itself. Transformations and projects that don't produce the results you want. These stumbling blocks and others remain in the way of cybersecurity that's truly trustworthy.

In the 2023 playbook, we identified critical challenges that C-suite executives should address together, as partners. These are still relevant.

Regulations that could change cybersecurity

The top initiatives in this chart are cyber-focused; the bottom, business-focused

Q10. To what extent is your organisation implementing or planning to implement the following cybersecurity initiatives?
Base: All respondents= 3876. Analysis technique utilised is factor analysis
Source: PwC, 2024 Global Digital Trust Insights.

In 2024, we're raising the challenge:

Do you dare, as a C-suite leader, to break out of the stasis and make the one or two bold moves that will matter most for your organisation?

Or to take that one imaginative leap that could finally clear the hurdles blocking your company from its goals?

We see some enterprises already picking their best bets. The array of options is broad.

What's right for your organisation?

Speak a new language.

CISO CFO GC

Placing yourself at the epicenter of innovation means meeting your leadership teams where *they* are and helping them to overcome the intimidation they might feel regarding what you do. Using insider terms such as cyber landscape, attack surface and even zero trust can only further mystify those outside your profession.

Dare to talk about cyber in business-speak, tech-speak, finance-speak or everyday-speak. Speak to your customers, investors and business partners in annual security reports in ways that inform and engage. Using common vocabularies can help executives wrestle with the trade-offs, tensions and chaos that inevitably happen at the epicenter of innovation.

Try bold, new ways of managing cyber risk.

CISO CRO IA CCO COO

Use more sophisticated approaches to cyber-risk modeling such as scanning for threats using formulas specific to your company's sector, vision and strategy. Create a risk-linked performance incentive for every bonus-eligible employee in the company, to build a risk culture. Invent new ways to find and strengthen your weaknesses, perhaps with a modern bug bounty programme that incentivises independent security research. Finally procure and begin using a cloud-first, centrally managed identity solution to secure your business expansion goals.

Shape guardrails.

CISO CIO GC RA

Speak the language of trust, not just regulatory compliance. Involve yourself early and often for the better chance at influencing any new rules and ensuring that they boost, not hinder, business success. AI, the metaverse, cryptocurrency, privacy — these hot regulatory topics could well benefit from your experience and insights. Remember, regulators can feel as befuddled as anyone by the workings of cyber and tech.

Free your teams for creative thinking (automation, GenAI, managed services).

CISO CIO CTO CRO COO

Providing you with around-the-clock eyes is one benefit of automation, GenAI and managed services. Performing mundane chores so your teams don't have to is another.

Liberated from the tyranny of tedious tasks, your people may find time and space to ponder new cyber threats and create new ways to thwart evolving threats.

Welcome cyber into the boardroom.

CISO B CEO

Cyber tops the risk register in most companies and on many executive surveys. But is it a staple topic in your boardroom? Are you getting quality information not on cyber risks and controls, but also on how major strategic initiatives are furthering business and revenue growth? Security provides the underpinnings for everything the organisation does: finance, development, personnel, technology and other areas of the business you likely discuss every time you meet.

Looking your cyber programme squarely in the eye can be a daring move.

Think like the business owner.

CISO CEO

Business transformation is one thing. Cyber transformation is not another. They are the same. The CISO and CEO together need now embrace cyber as a whole-of-business endeavor, putting yourselves in the business owner's shoes. Wouldn't they want every aspect — financial records, proprietary research, application development, customer data and the like — protected from unauthorized viewing or use? Wouldn't they want to safeguard their brand? Couldn't cybersecurity spur innovations that save money and help the business to grow? This is the raison d'etre of cyber.

About the survey

The 2024 Global Digital Trust Insights is a survey of 3,876 business, technology and security executives (CEOs, corporate directors, CFOs, CISOs, CIOs and C-Suite officers) conducted in the May through July 2023 period.

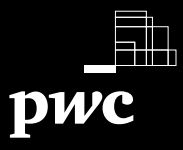
Four out of 10 executives are in large companies with $5 billion or more in revenues. Importantly, 30% are in companies with $10 billion or more in revenues.

Respondents operate in a range of industries, including industrial manufacturing (20%), financial services (20%), tech, media, telecom (19%), retail and consumer markets (17%), energy, utilities, and resources (11%), health (9%) and government and public services (3%).

Respondents are based in 71 countries. The regional breakdown is Western Europe (32%), North America (28%), Asia Pacific (18%), Latin America (10%), Eastern Europe (5%), Africa (4%) and Middle East (3%).

The Global Digital Trust Insights Survey had been known as the Global State of Information Security Survey (GSISS). In its 26th 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 to learn more

Sean Joyce
Global Cybersecurity & Privacy Leader,
US Cyber, Risk & Regulatory Leader
PwC US
sean.joyce@pwc.com | LinkedIn