Global Risk Landscape 2026

Risk Everywhere

Extending ownership beyond the risk function

PRÓLOGO

Vivimos en un presente donde la globalidad y la evolución constante provocan que los riesgos emerjan y muten de manera vertiginosa: geopolítica, ciberseguridad, IA, etc.

Gonzalo García-Liñán
Socio responsable de Risk Advisory Services, BDO España
gonzalo.garcia-linan@bdo.es

Los cambios constantes que se producen a nivel global implican que las empresas ya no pueden limitarse a quedarse al margen y esperar a que mejoren las condiciones: deben estar preparadas para actuar con decisión y asumir riesgos calculados incluso cuando el futuro a corto plazo sea incierto. El problema radica en que muchas organizaciones siguen aplicando un enfoque de gestión de riesgos demasiado reactivo y teórico, lo que limita su eficacia.

Los mandos directivos de las grandes corporaciones reconocen, por un lado, la preocupante e incierta coyuntura actual y, por otro, la importancia de gestionar los riesgos de forma rápida y proactiva. Sin embargo, en la práctica, a muchos les cuesta actuar con mayor rapidez porque la gestión de riesgos sigue estando en manos de equipos especializados que trabajan de forma aislada, lo que limita el campo de visión y ralentiza la velocidad de la toma de decisiones.

Este informe analiza cómo la gestión del riesgo transversal puede impulsar mejores resultados y proporcionar a las organizaciones la confianza necesaria para asumir riesgos de manera proactiva en los ámbitos donde más valor aportan.

8 /10

de los líderes empresariales afirma que el panorama global de riesgos está hoy más que nunca definido por las diferentes crisis globales que estamos viviendo de manera continua.

52%

de los líderes empresariales señala que tiene dificultades para identificar qué señales de riesgo son realmente relevantes frente al ruido de fondo.

Contents

Executive summary	05
Embracing confidence in an era of uncertainty	06
Geopolitics: The risk shaping all others	12
How business leaders are responding to disruption	16
Cyber: The number one risk without a clear plan	19
Fraud: The misunderstood risk under a technology illusion	23
AI: From hype to practical application, with uneven control	26
Ushering in risk management that acts, not reacts	30
Methodology and demographics	31
Contributors	32

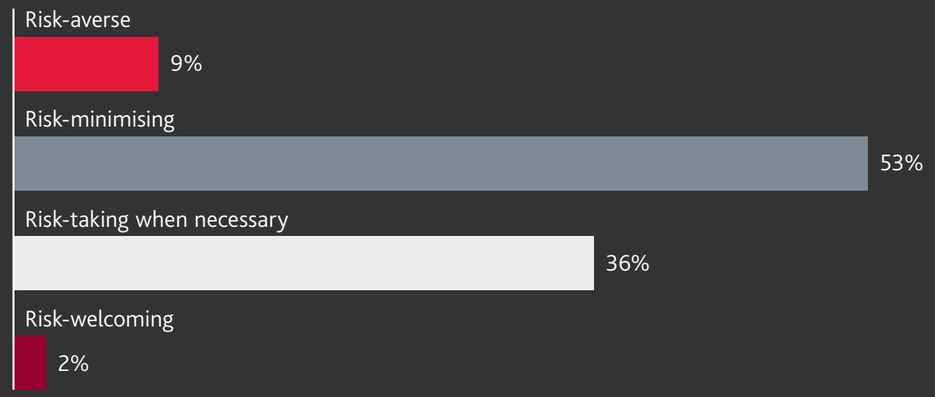
Executive summary

Embracing confidence in an era of uncertainty

Uncertainty is now structural. Businesses that remain in protective mode are in danger of being overtaken by those willing to make calculated risk decisions.

See page 06

How business leaders categorise their risk appetite in 2026



Geopolitics: The risk shaping all others

Geopolitics is no longer one risk among many: it is the multiplier that amplifies supply chain, cyber, and regulatory exposures. Leadership teams are divided on which consequences matter most, which is itself a risk.

See page 12

Geopolitical risk is a

top-three risk that business leaders feel unprepared for

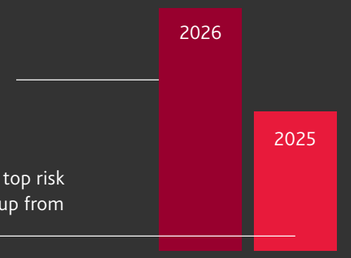
Cyber: The number one risk without a clear plan

Cyber is now the top risk that businesses are unprepared for, according to two in five business leaders. Spending is rising, but attacks are rising faster. Meanwhile, cyber teams are routinely brought into transformation initiatives too late, with only 10% involved at the ideation stage.

See page 19

40%

of leaders cite cyber as a top risk they are unprepared for, up from 23% in 2025



Fraud: The misunderstood risk under a technology illusion

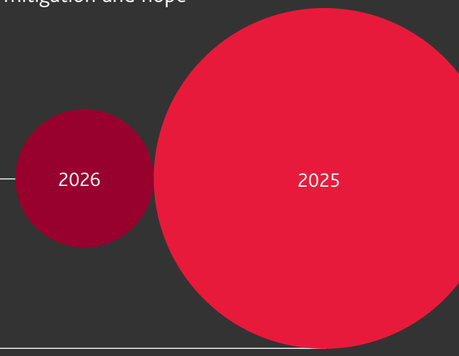
Fraud is falling off the agenda: 93% of leaders don't see it as a top risk, and just 13% are actively updating their defences (down from 79% last year). Business leaders can't afford to deprioritise fraud mitigation and hope technology catches up.

See page 23

13%

are actively monitoring and updating defences against AI-enabled fraud, down from

79% last year



AI: From hype to practical application, with uneven control

AI optimism is growing. But as pilots move into live deployment, governance gaps are widening. AI amplifies existing weaknesses in data, controls and compliance, rather than correcting them.

See page 26

Top five AI risks according to business leaders

Survey of 500 C-suite executives worldwide conducted December 2025–January 2026. Full details at page 31.

Embracing confidence in an era of uncertainty

Why shared ownership needs to be the new approach to risk

At a glance

What is changing

Persistent volatility and the breakdown of geopolitical and institutional norms are upending traditional risk management models

Why it matters

Corporate survival is on the line

What to do

Treat risk management as a strategic enabler, not a defensive function

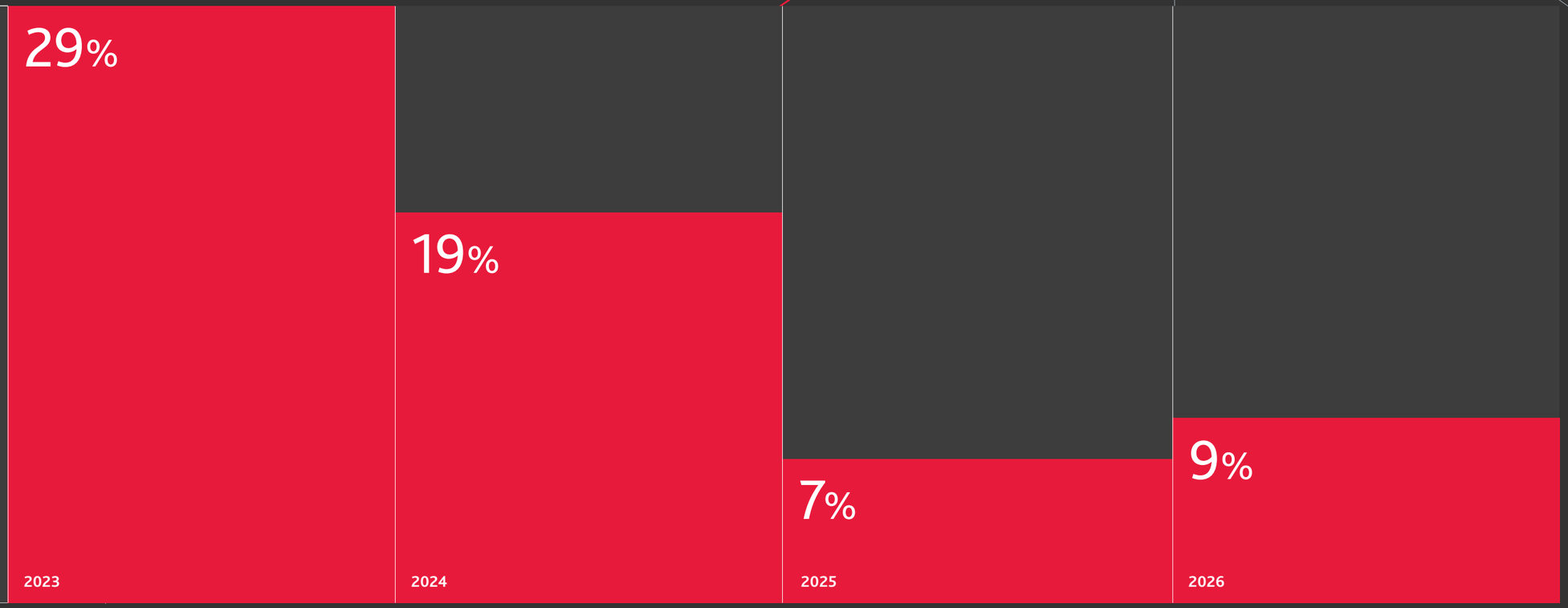
The cost of standing still in times of crisis is no longer just a case of missing new business opportunities. For many businesses, this is now about their long-term survival.

More than two thirds of business leaders (68%) agree that the speed at which crises are impacting their organisations is increasing, up from 54% a year ago.

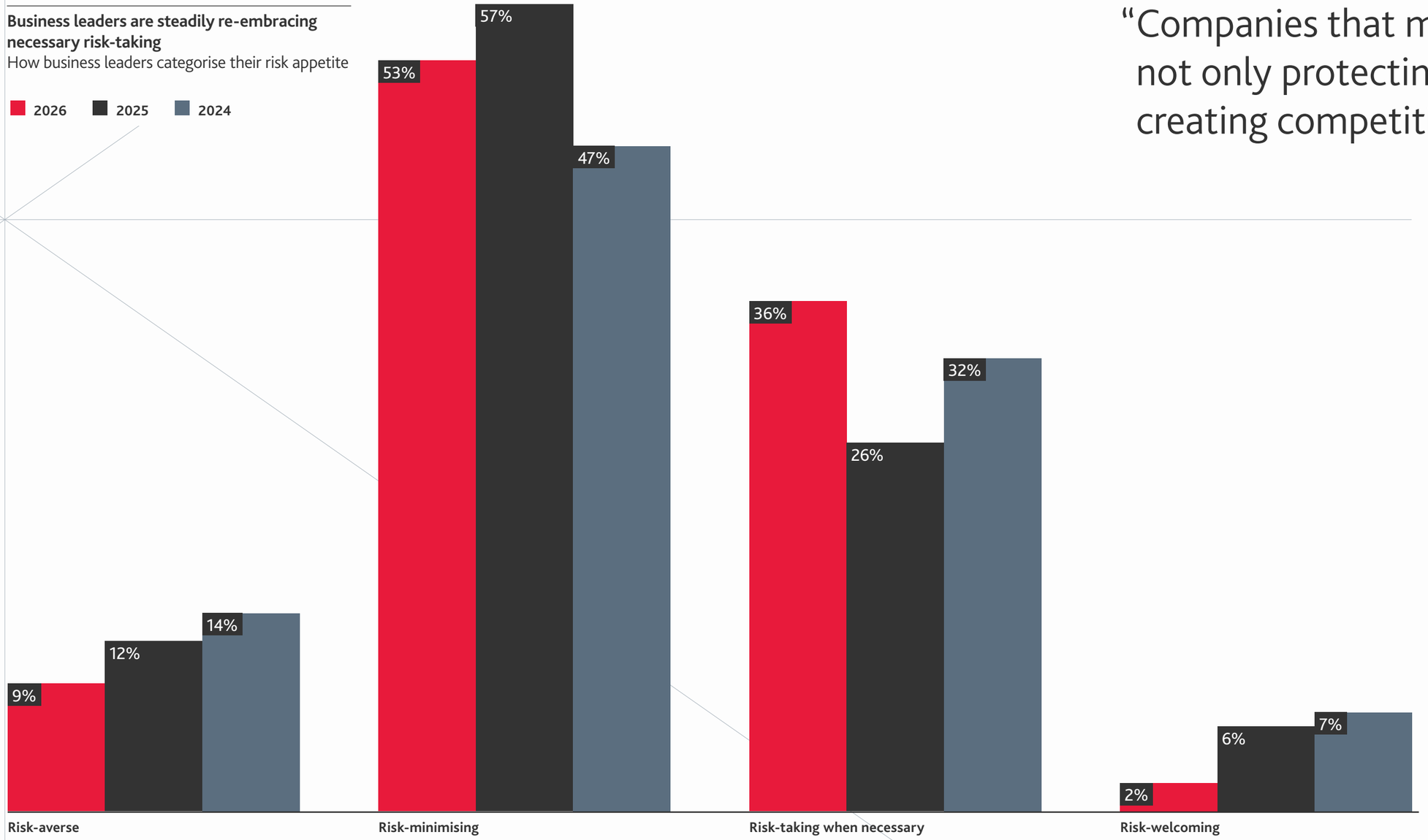
The risk of inaction is not solely driven by the frequency of crises either. It is equally shaped by the pace of change in the world at large, accelerated by forces such as AI. Amid this instability, organisations increasingly recognise that traditional risk management approaches are not fit for purpose: to survive, they need to take more calculated risks.

"For some businesses, this is existential," says Alisa Voznaya, Partner and Head of Risk Consulting at BDO UK. "If they don't take the risks now, there won't be a business. So those organisations that have typically been risk averse are having to revise their approach, otherwise they're just not going to be around in the future."

Proactive risk management is becoming less common
Percentage who say their risk management is "very proactive"



Business leaders are steadily re-embracing necessary risk-taking
How business leaders categorise their risk appetite



"Companies that manage risk well are not only protecting their assets, but creating competitive edge."

That existential risk is being compounded by a raft of issues that are landing at the same time: supply chain disruption, intensifying competition and an increased regulatory burden. On their own, the risks may be manageable. But when they happen all at once, their interaction means they can "kill your business immediately," says Voznaya.

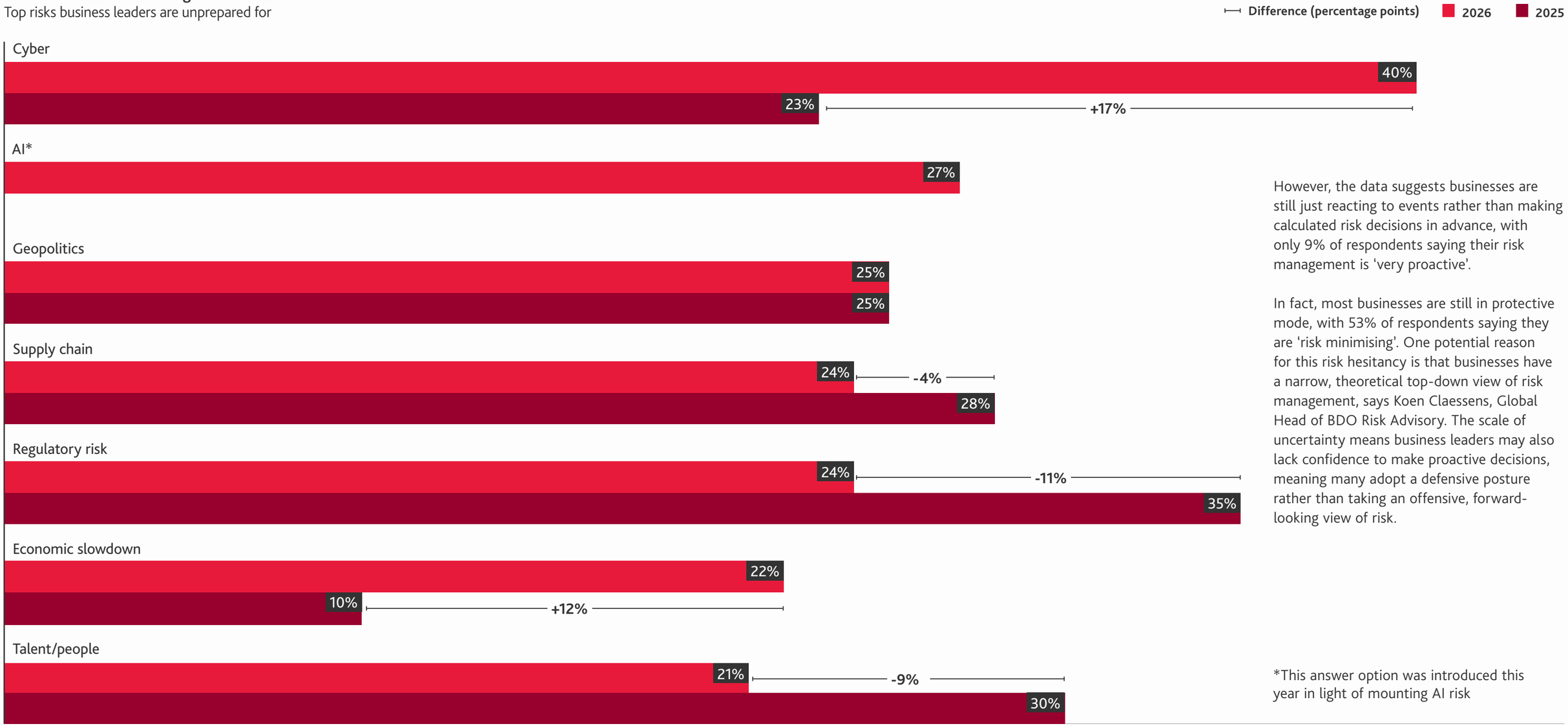
Other businesses are starting to realise that you can't wait for a crisis to hit and then respond, adds Voznaya: they know they must start anticipating the potential risks (and opportunities) on the horizon.

The data shows that a growing cohort of businesses are adopting a more calculated risk approach, with 36% of business leaders saying they are now risk-taking when necessary, compared to 26% a year ago.

"I think companies that manage risk well are not only protecting their assets, but creating competitive edge," says Matteo De Renzi, CEO at the ride-hailing platform Gett.

Tech-based risks are creating more concern

Top risks business leaders are unprepared for



However, the data suggests businesses are still just reacting to events rather than making calculated risk decisions in advance, with only 9% of respondents saying their risk management is 'very proactive'.

In fact, most businesses are still in protective mode, with 53% of respondents saying they are 'risk minimising'. One potential reason for this risk hesitancy is that businesses have a narrow, theoretical top-down view of risk management, says Koen Claessens, Global Head of BDO Risk Advisory. The scale of uncertainty means business leaders may also lack confidence to make proactive decisions, meaning many adopt a defensive posture rather than taking an offensive, forward-looking view of risk.

*This answer option was introduced this year in light of mounting AI risk

"Business leaders need to find the right dose of risk management versus going into hibernation mode because there's too much risk around you – otherwise, it impairs growth," says Johanna Pudda, CEO at supply chain and warehouse business Staci Americas.

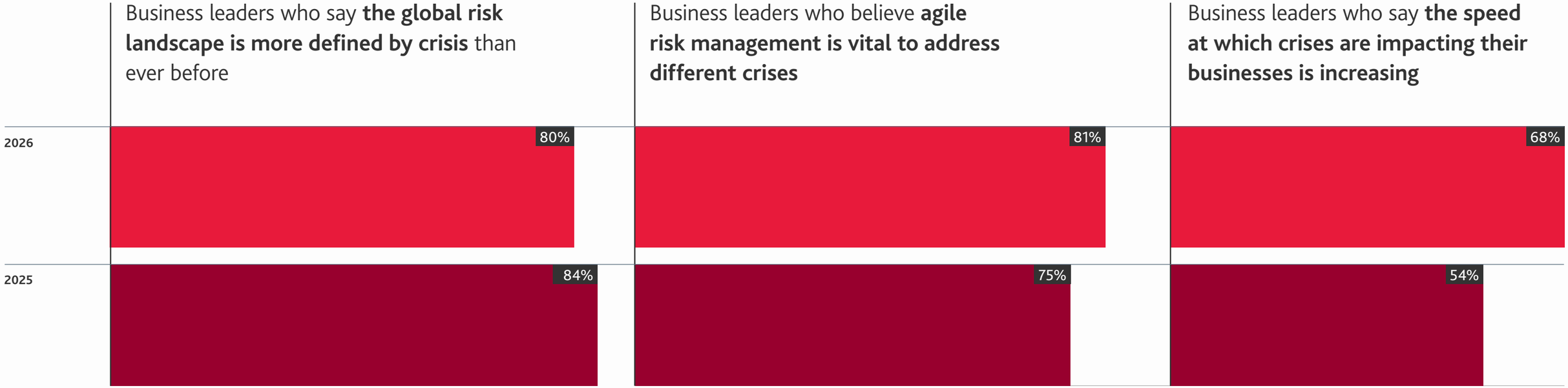
This doesn't mean organisations need a greater risk tolerance. It simply means there must be a clearer, shared view of how risk decisions will impact the wider business.

One key challenge is that businesses are often bogged down by day-to-day operating issues. Some 55% of business leaders say that short-term operational pressures frequently override their long-term or predictive risk planning, while 52% say they struggle to identify which risk signals truly matter versus background noise.

"Organisations may find it very difficult to foresee the kind of risk that they're facing, especially when it's something they've not had on the radar screen before or if it's outside their control," says Ricky Cheng, Director and Head of Risk Advisory at BDO Hong Kong.

"Organisations don't need greater risk tolerance. There must be a clearer, shared view of how risk decisions will impact the wider business."

Crisis is now the baseline and agility is seen as essential



Competing and overwhelming priorities are a growing problem

55%

of business leaders say that short-term operational pressures frequently override their long-term or predictive risk planning

52%

say they struggle to identify which risk signals truly matter

Yet the challenge is not just identifying those risk signals: it is about managing those risks in a joined-up way. This is a frequent stumbling block because risk management is often viewed as a specialist discipline and not a shared responsibility across functions. This creates a widening divide between organisations that can define their risk position with the confidence to make more agile risk decisions and those that struggle because they lack a coherent view of risk across the business. In this environment, the ability to act with some level of certainty (even if it is incomplete) becomes a competitive advantage.

To achieve this, risk management must shift from a defensive function to a strategic capability. Organisations therefore must define their appetite for risk taking and where to focus on risk mitigation. This means identifying risk management opportunities and not just battening down the hatches as an auto-response to disruption.

"If you don't understand your risk position you end up not moving, and not moving is also a decision," says Richard Liao, CEO of Taiwanese glass bottling business Hwa-Hsia Glass. "It means your competitors are the ones that are going to take the opportunities you're not."

INSIGHT

Risk isn't a barrier. Standing still is

Why the case for cautious risk management no longer holds

Alisa Voznaya

Partner and Head of Risk Consulting at BDO UK

Over the past few years, businesses have taken a more risk-minimising or even risk-averse approach to managing their operations, hoping to "get to it when things get better". Time has run out for this mindset: companies have come to a realisation that it's no longer possible to sit on their hands and expect positive outcomes.

Many businesses now recognise that it is essential to take calculated risks. There are two parallel streams to this. One is the business model survival route: the idea that companies have to change not to thrive, but simply to survive. The other is a more forecasting-heavy view of risk where you look to identify pockets of vulnerabilities and opportunities.

It's a different world now. From a strategic perspective, the time-tested rules and norms are no longer applicable. And if the rule book has been ripped up, the old processes aren't going to work. You must think in an innovative way to rise to the challenge.

Geopolitics: The risk shaping all others

Why no single function can manage geopolitical risk on its own

At a glance

What is changing:

Geopolitics is becoming even more unpredictable and volatile

Why it matters:

Geopolitics cuts across all risks, amplifying other exposures and acting more as a causal factor

What to do:

Bring together cross-functional viewpoints to understand collective business impacts

"Geopolitical risk used to be a discrete concern. Now it's becoming the primary risk multiplier that we're all concerned with," says Richard Walker, Head of Risk Advisory Services at BDO South Africa.

Geopolitical risk is increasingly recognised as unique because it cuts across all other risks, amplifying supply chain, regulatory and cyber vulnerabilities. With the backdrop becoming even more volatile and the impacts even more pronounced, businesses are starting to rethink how they manage geopolitical fallout.

However, while leaders are aligned on the scale of the threat, they have disparate views on the potential impacts. CEOs, for example, believe the main impact will be fragmented supply chains, while tech leaders believe the biggest threat is regulatory divergence. Meanwhile, CFOs think cyber-related geopolitical threats will be the biggest consequence.

This underscores why businesses need a shared, coherent and agile approach to risk management that considers cross-functional viewpoints. As Gonzalo García-Liñán, Risk Advisory Services Partner at BDO Spain, explains: "Risk does not affect every part of a business in the same way: it lands differently in a finance department than it does in operations or technology, for example. The best way to manage risks is to give a voice to everyone involved. If anyone is left out, there will be a crucial perspective that is not taken into account."

"What we're dealing with is the uncontrollable," says Johanna Pudda of Staci Americas. "That's where the agility of the organisation matters, the structure underneath, and how resistant and resilient your company is to these types of uncontrollable risks today."

The real challenge is understanding how risks interact and managing competing demands across resilience, cost, speed and market access. Ziad Akkaoui, Partner and National Risk Advisory Practice Leader at BDO Canada, puts it plainly: "Organisations make better decisions when they stop treating this as a coordination problem and start treating it as a decision model issue. Risk, operations, technology and finance need to come together early, with clear decision rights, common scenarios and an agreed view of the trade-offs involved."

Regional priorities differ, but the underlying pressure of geopolitical risks are the same
Geopolitical threats to organisations by region (next 12-18 months)

	Europe	Middle East	Africa	APAC	Americas
#1	Fragmentation of supply chains	Cross-border tech/ data restrictions	Regulatory divergence	Fragmentation of supply chains	Cyber-enabled geopolitical threats
#2	Regulatory divergence	Regulatory divergence	Cyber-enabled geopolitical threats	Regulatory divergence	Regulatory divergence
#3	Cyber-enabled geopolitical threats	Fragmentation of supply chains	Unpredictable tariff changes	Cyber-enabled geopolitical threats	Cross-border tech/ data restrictions

Geopolitical risk is a **top-three risk** that business leaders feel unprepared for this year

Leaders are aligned on the scale of the threat, not the specific danger
Geopolitical threats to organisations by job role (next 12-18 months)

	CEOs	Tech leaders	CFOs
#1	Fragmentation of supply chains	Regulatory divergence	Cyber-enabled geopolitical threats
#2	Regulatory divergence	Cross-border tech/data restrictions	Cross-border tech/data restrictions
#3	Regional political instability	Cyber-enabled geopolitical threats	Diplomatic tensions affecting talent mobility etc

"The goal is not to wait for perfect information, but to create enough alignment, early enough, to move decisively.

"The goal is not to wait for perfect information, but to create enough alignment, early enough, to move decisively. That is what democratising risk really looks like in practice: broader ownership, faster judgement and better enterprise-level decisions," says Akkaoui.

These choices are too consequential to sit within a single risk function, which is why coordinated decision-making across teams has become so important.

Crucially, organisations must define their appetite for risk. This means building a clear understanding of existing threats. More than that, it involves determining which risks are acceptable to carry, which require mitigation, and which demand immediate action.

In this environment, risk is no longer a sporadic, isolated event. It is the new operating model that will determine whether businesses can survive and thrive in an increasingly unstable world.

Geopolitics is forcing businesses to think differently on risk

Erin Sells
Principal, Risk Advisory Services
at BDO USA

Stronger responses require diverse voices

To combat risk is to consider the range of viewpoints across functions, recognising there are different leadership styles across different countries.

Today more than ever, there are many different perspectives that need to be brought into risk planning in a way that hasn't been done before. It's about ensuring that all functions have a voice at the table and a chance to weigh in on how companies address risk.

Richard Walker
Head of Risk Advisory Services
at BDO South Africa

Why waiting is not an option in geopolitical risk

The faster geopolitical risks escalate, the earlier business leaders need to start making calls on where they're exposed, which sometimes means making decisions based on incomplete data.

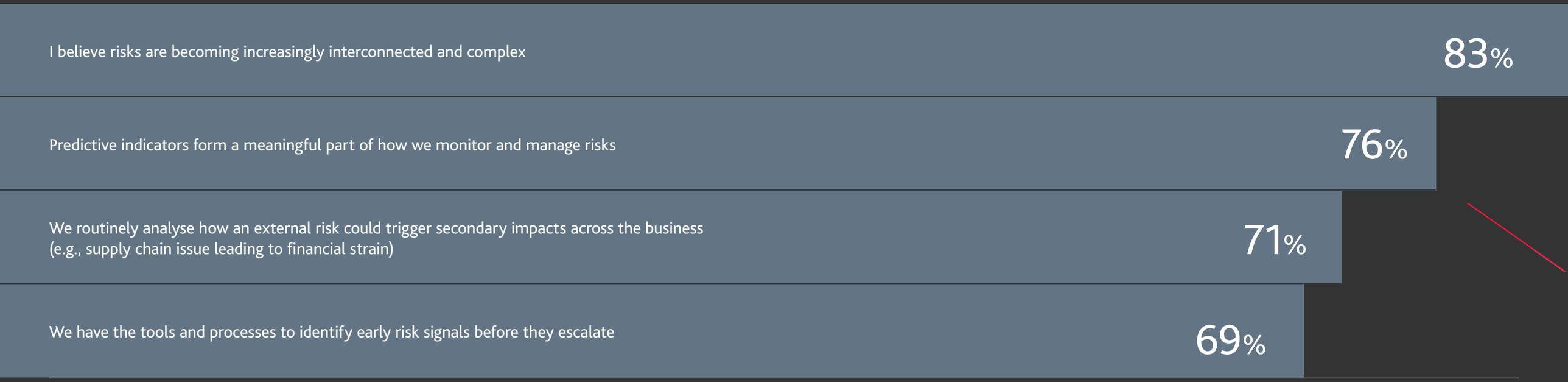
If the data or intelligence you receive is rushed and incomplete, scenario planning becomes essential to mitigate against that and determine whether the balance sheet can handle the decision.

How business leaders are responding to disruption

Organisations know that risks are multiplying and becoming more interconnected. But awareness alone is not enough. Our findings reveal where the real gaps lie and what business leaders are doing to close them.

89% consider the interdependencies between risks (e.g., geopolitical, supply chain, cyber, economic) when assessing threats

Business leaders recognise how risks influence one another and are reflecting this in their risk management



But there are still efficiency gaps
The top risk management challenges identified by business leaders

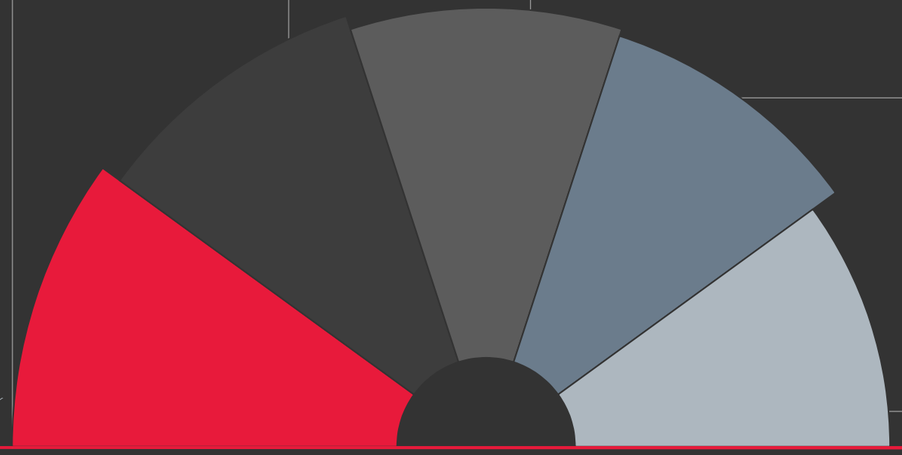
55%
Short-term operational pressures frequently override long-term or predictive risk planning

52%
We struggle to identify which risk signals truly matter versus background noise

50%
Risk information remains siloed across departments or functions

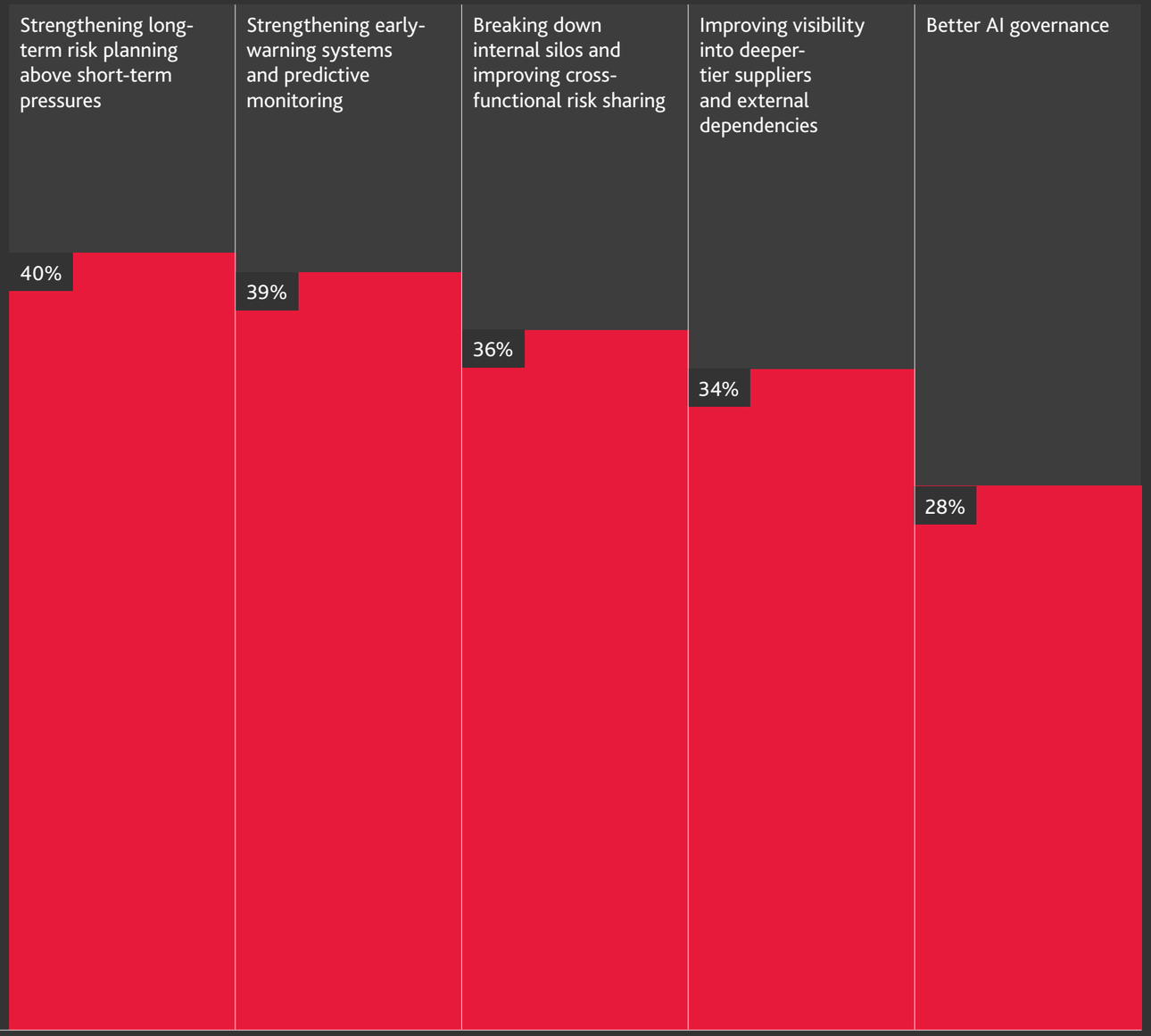
49%
We lack consistent early-warning indicators to act before risks materialise

45%
We have limited visibility into deeper-tier suppliers and external dependencies

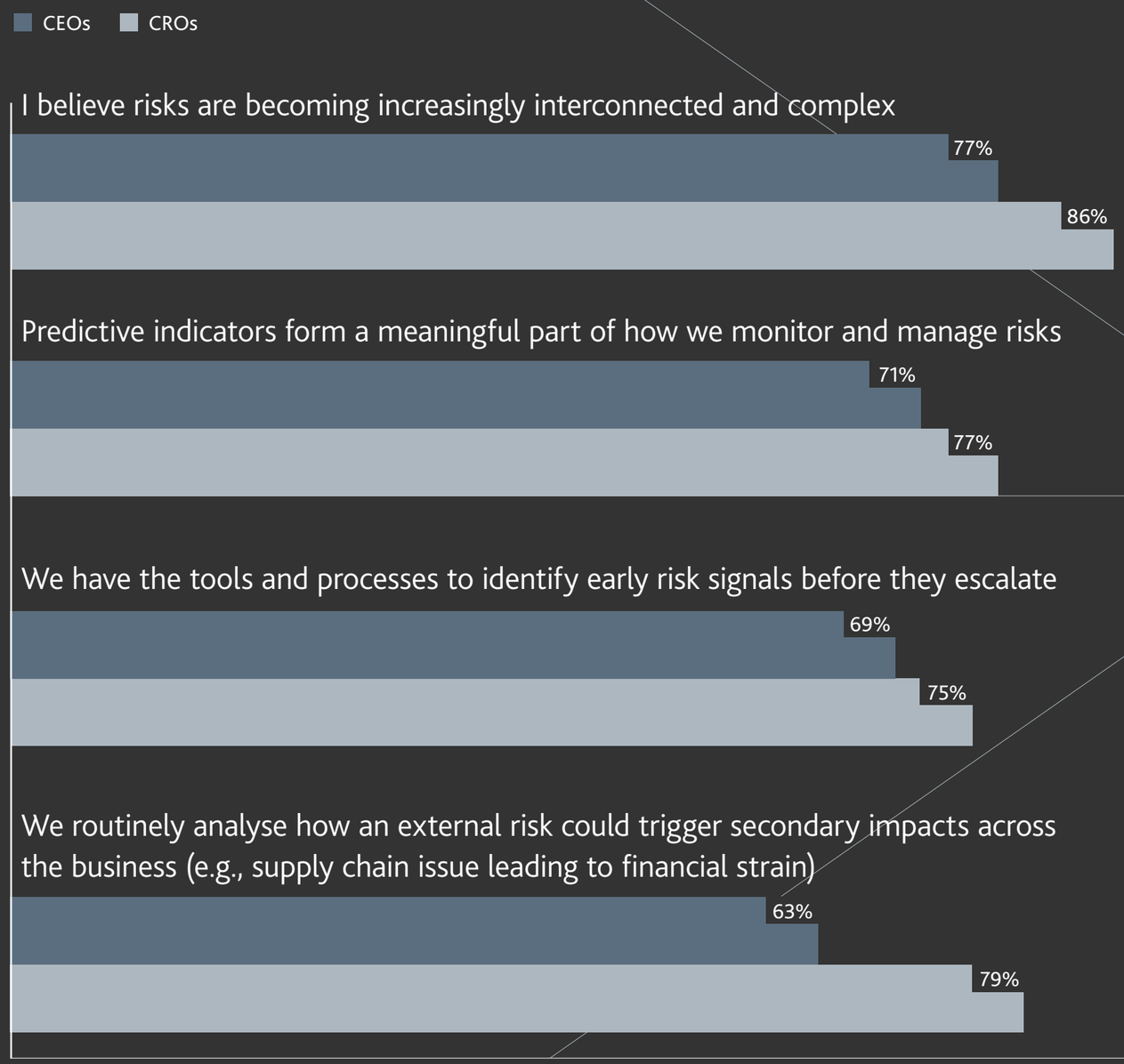


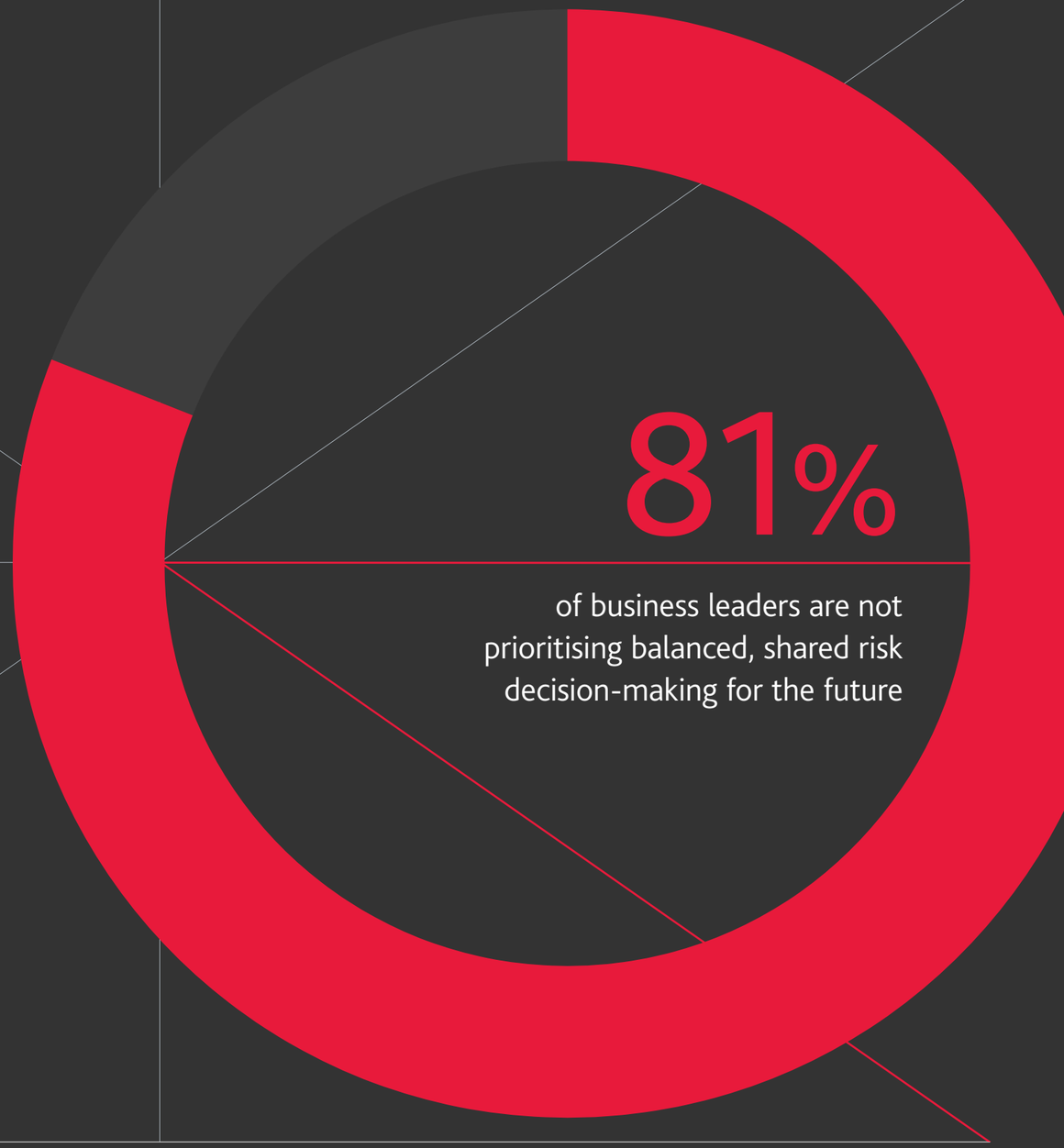
99% are prioritising some form of risk management improvements for the next three years

While there's a clear desire and action to close these gaps...
The risk management improvements organisations are prioritising for the next three years



...leadership teams are not yet fully aligned on the extent of the problem





Cyber: The number one risk without a clear plan

Growing threats are exposing the limits of traditional cyber defence strategies

At a glance

What is changing:

Cyber attacks keep on rising despite ever-increasing cyber defence spending

Why it matters:

Tech transformation is accelerating. Cybersecurity needs to keep up

What to do:

Worry less about blanket protection. Instead target broader resilience

Organisations are spending ever greater sums on cybersecurity. It isn't slowing down the rate of attacks.

The average number of weekly attacks grew 58% globally between 2023 and 2025, according to the World Economic Forum,[1] with that threat lifting cyber risk back to the number one risk business leaders say they are unprepared for.

Part of the challenge is that legacy methods of cyber risk management can no longer keep pace with the rapid evolution of technology and the capabilities that it brings. This is either due to organisational resistance or because cyber teams are not introduced early enough in the transformation cycle, says Rocco Galletto, Partner and Global Cybersecurity Leader at BDO Canada.

While many cyber teams are brought in during the planning stage of transformation initiatives (57%), only 10% are involved during ideation and 26% have to wait until the execution phase.

The threat backdrop is also evolving faster than cyber risk management can keep up, with cyber criminals taking advantage of new technologies. Unlike businesses that must go through multilayered procurement and approval processes, hackers can immediately start using the technology.

Business leaders aren't entirely confident in their cyber investment

23%

CEOs say their business is underspending on cybersecurity

1. Cybersecurity awareness: AI threats and cybercrime in 2025 | World Economic Forum

Organisations must accept that what worked in the past will not work in the future.

"There are a lot of issues with software or things that can be exploited in software, and AI is going to present the opportunity to exploit those before any organisations realise there's even any threat," says John Messina, IT consultant and former CIO of the Canadian government.

Business leaders are also divided on how cyber risk will evolve. While 35% of CEOs and tech leaders agree cyber is the top risk today, only 29% of CEOs think it will remain a top risk over the next five years, compared to 41% of tech leaders.

This discrepancy hints at a false sense of security that cyber will always keep pace with business and technology transformation.

"Organisations are not operating in that way, and with technology being implemented faster now, this introduces more risk," says Galletto.

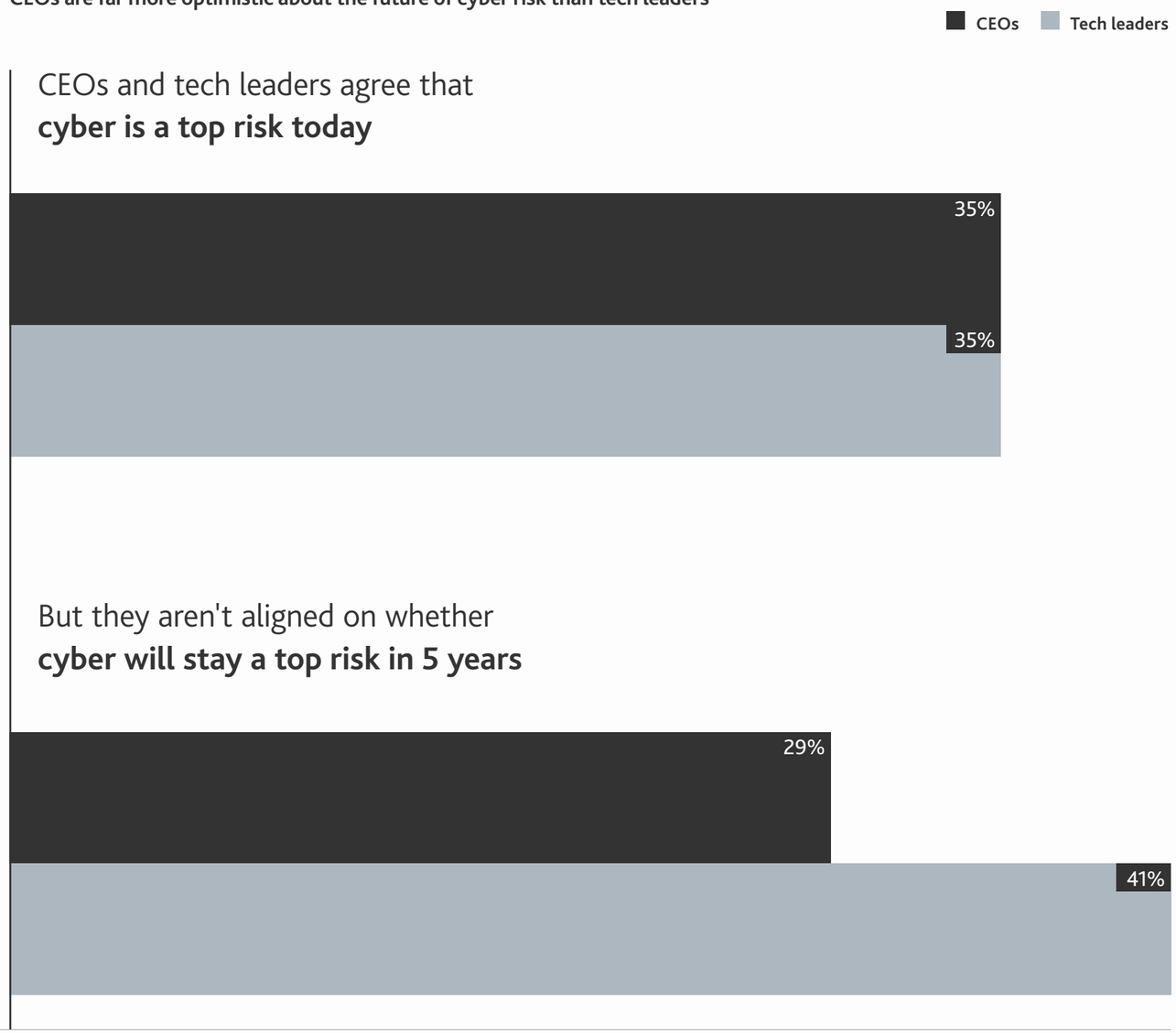
While most organisations believe they spend enough on cyber defence – only 23% of CEOs say their business is underspending on cybersecurity – figuring out the right level of investment remains a challenge.

"If you're in continuous transformation, you probably should be spending more to keep pace," says Galletto. "If you're below your industry cyber spending benchmark, you're likely not spending responsibly."

With cyber attacks continuing to increase, business leaders are left to ponder whether it is because cyber spend isn't increasing fast enough to mitigate the risk or whether it is because they are hamstrung by legacy processes, adds Galletto. Either way, organisations must accept that what worked in the past will not work in the future. Cyber strategies must change to fit this new era of risk.

In practice, this involves a more dynamic strategy that ensures cyber spending keeps pace with tech transformation, while focusing on resilience and response in a more targeted way. Humans remain the weakest link in an organisation's cyber defences, so the strategy must also ensure cross-functional individual accountability.

CEOs are far more optimistic about the future of cyber risk than tech leaders

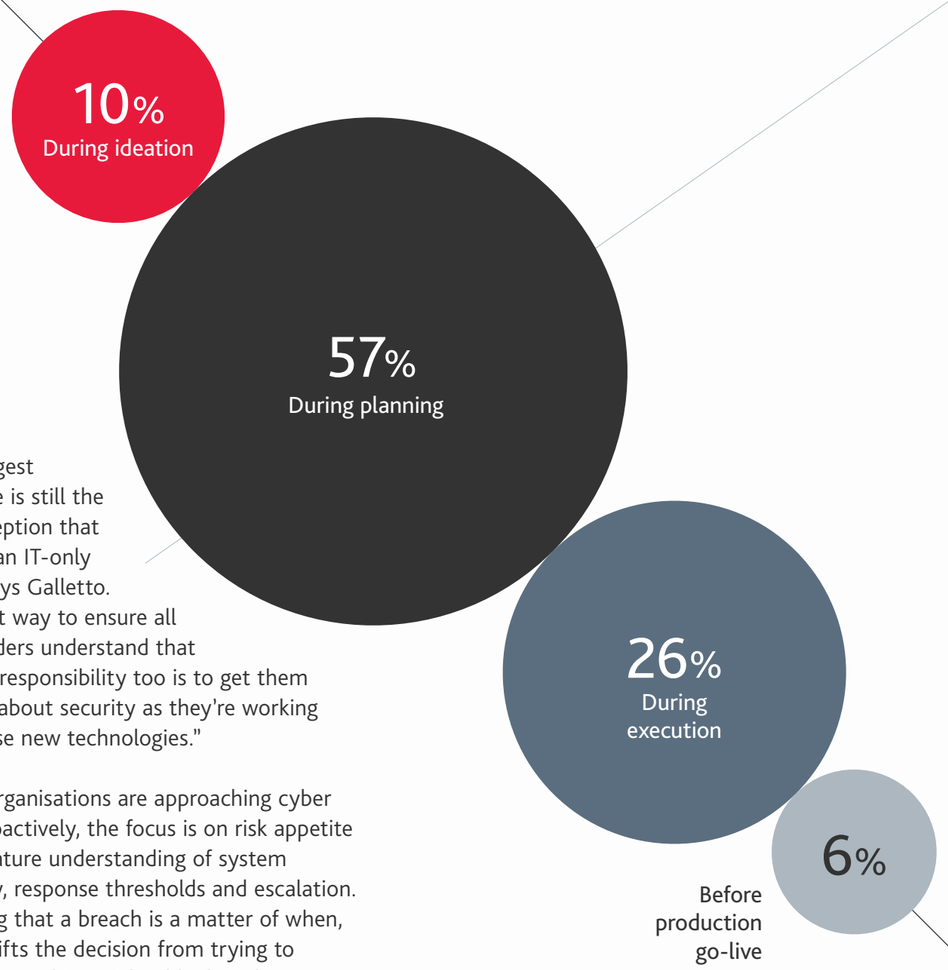


Cyber action still centres on response and compliance
The top five cybersecurity priorities for businesses over the next two years

#1	#2	#3	#4	#5
Improving threat detection	New compliance measures	Enhancing data protection privacy	Upgrading incident response plans	Preparing for AI-driven risks
53%	52%	49%	48%	46%

Incident response and AI are gaining ground but training is taking a backseat
Top three actions business leaders will take in the next two years to reduce cyber risk

And cyber teams are often being asked to secure decisions that have already been made
When cyber teams typically get involved in transformation initiatives



"The biggest challenge is still the misconception that cyber is an IT-only issue," says Galletto. "The best way to ensure all stakeholders understand that it's their responsibility too is to get them thinking about security as they're working with these new technologies."

Where organisations are approaching cyber more proactively, the focus is on risk appetite and a mature understanding of system criticality, response thresholds and escalation. Accepting that a breach is a matter of when, not if, shifts the decision from trying to protect everything with a blanket plan to more strategic planning around resilience.

INSIGHT

Don't treat cyber as an afterthought

Cyber teams need a seat at the table from day one

Rocco Galletto
Partner and Global Cybersecurity Leader at BDO Canada

The ideal stage for cyber teams to get involved in business transformations is at ideation, when you're first defining the strategy and direction. There's a good reason for this: it allows you to anticipate likely threats and build security in from the start. Get involved too late and you end up playing catch-up forever, and at the pace businesses move today, you never catch up.

The challenge is that businesses don't always understand the value of having cyber at the outset, or why it should be a strategic enabler rather than a last-minute add-on before go-live. Because if you go live without having built security in, threat actors have the entire product lifecycle to find a way in.

Fraud: The misunderstood risk under a technology illusion

Fraud deserves more executive attention than it is currently getting

At a glance

What is changing:

Business leaders are less concerned about fraud risk

Why it matters:

Sophisticated, AI-powered fraud is on the rise

What to do:

Invest in AI tools to improve fraud detection and prevention

AI-powered deepfake technology is enabling fraudsters to automate scams at scale, increasing fraud risk for businesses. Yet alarmingly, fraud is slipping down the executive agenda. Some 93% of business leaders don't rank fraud as one of the major threats they're unprepared for, suggesting a serious case of downplaying the threat.

Part of the reason fraud has become a lower priority is not because fraud has reduced, but because the enforcement backdrop has eased, particularly in the US. This then tends to permeate across other large economies, says Glenn Pomerantz, Principal & Forensic Leader at BDO USA and Global Forensic Leader.

"When enforcement is down, it's just not front of mind for executives," says Pomerantz.

Another explanation is simply that fraud is being bundled into other risk factors – notably cyber and AI – which were the top two risks reported by businesses this year.

"When you carve out AI, cyber and things like digital asset-related fraud, what you are left with is the more mundane generic-type frauds that are really more like yesterday's frauds," says Pomerantz.

While businesses are aware of AI fraud risk – 79% of business leaders said they had a plan in place to defend against AI-driven fraud last year – just 13% this year say they are actively monitoring and updating their defences specifically for AI-enabled fraud. Given how fast the underlying tech is evolving, organisations that don't take a more dynamic approach to AI fraud risk will become increasingly vulnerable.

Fraud is a threat that's still largely misunderstood

93%

of business leaders don't believe that fraud is a top risk for their organisation

79%

of business leaders said they had a plan to defend against AI-driven fraud in 2025

Just 13%

are actively monitoring and updating their defences specifically for AI-enabled fraud in 2026

"Everybody is focused on AI governance, but in terms of AI fraud prevention, businesses are lagging," says Pomerantz. "The criminals will be moving faster, so you're going to constantly have to revise and enhance your fraud defences."

Right now, businesses are focusing broader fraud risk mitigation efforts on staff training, but that will shift over the next two years, with most business leaders expecting their organisations to increase their use of AI to identify fraud.

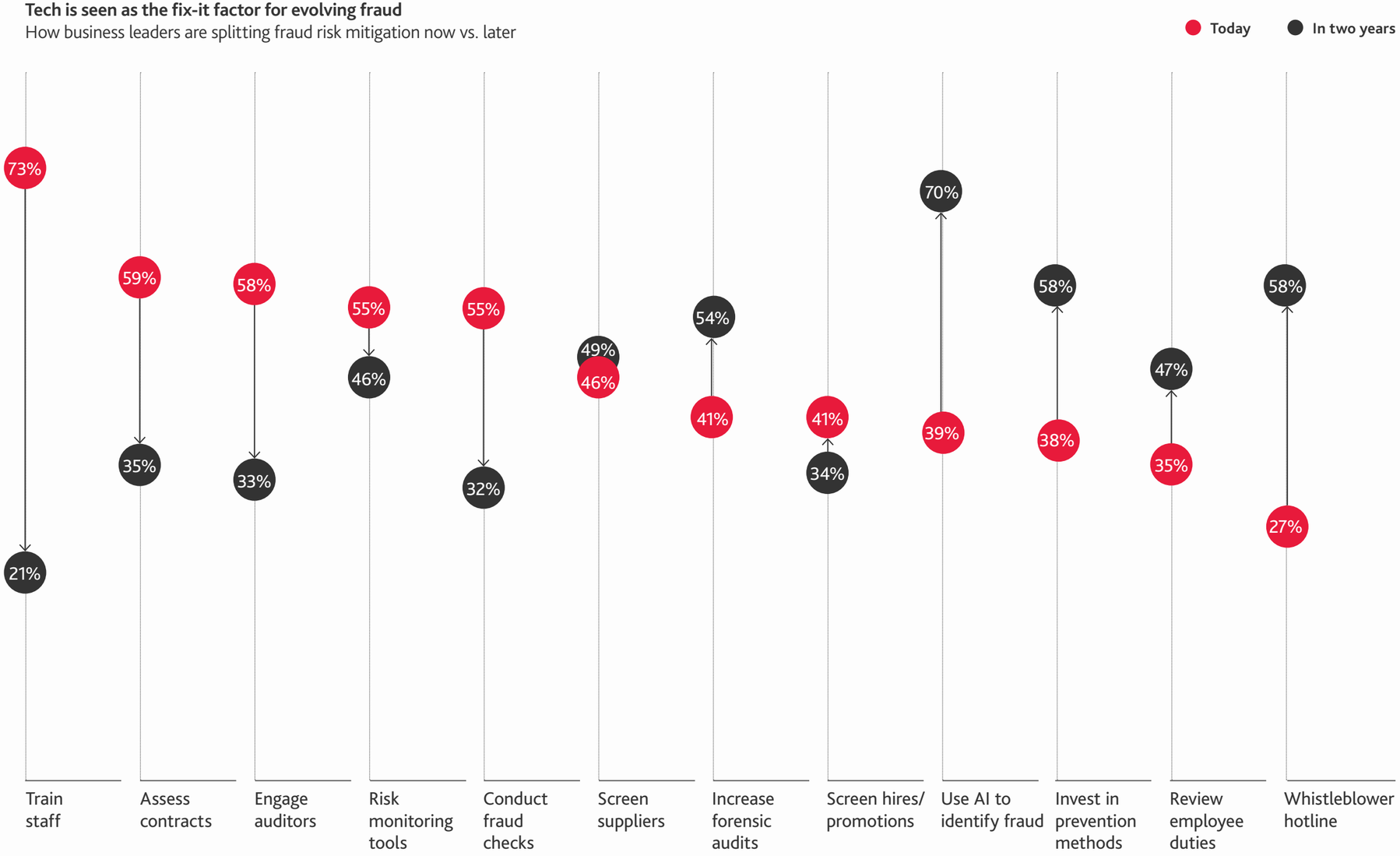
There is a snag. By waiting for advanced AI tools to combat fraud rather than redesigning controls to align to today's threats, organisations are likely to remain in reactive mode. That means fraud will only rise up the risk agenda when (not if) fraudsters successfully target the business. This echoes early attitudes towards cyber risk, where senior leadership teams failed to see the benefits of investing in cybersecurity until they suffered a cyber incident, says Richard Liao of Hwa-Hsia Glass.

"It takes some patience and time for people to really see the force of a problem coming to them before they jump on board," Liao adds.

With AI and cyber-driven fraud elevating risk, business leaders must reprioritise and revamp their approach to fraud mitigation today and not just hope that tech will provide a better solution in the future.

Tech is seen as the fix-it factor for evolving fraud

How business leaders are splitting fraud risk mitigation now vs. later



Fraud risk is rising in a more volatile world

Glenn Pomerantz
Principal & Forensic Market Leader at BDO USA

Where AI tools can mitigate fraud risk

Our data shows AI fraud mitigation tools will be more commonly used in two years rather than now, likely due to the budget required and the need for proper staff training. These solutions also need to be customised for your business rather than taken off the shelf.

But third-party due diligence is a good example of where AI is starting to play a role. If you're already using AI for investigative work in global corporate intelligence, the next step is applying it to compliance and vetting third parties. We may also see it emerge in C-suite recruitment and checks, where businesses need to avoid the embarrassment of hiring a CFO or CEO with skeletons in the closet or relationships incompatible with the business.

Markus Brinkmann
Partner and Head of Forensic, Risk & Compliance at BDO Germany

Fraud prevention is becoming increasingly dynamic

Today's geopolitical challenges are creating volatility and uncertainty across the global economy, dramatically increasing the likelihood of fraud. Businesses are operating in an environment where factors such as disrupted supply chains, geopolitical tensions, climate change and shifting regulatory pressures are making risks harder to predict and more difficult to monitor consistently. At the same time, organisations are relying on increasingly complex systems and digital processes that can create additional vulnerabilities if governance does not keep pace.

Risks cannot be treated as static anymore. In a volatile environment, businesses need to identify and reassess risks continuously because threats can evolve very quickly, particularly as fraud tactics become more sophisticated and technology-driven.

AI: From hype to practical application, with uneven control

Why AI governance must keep pace with AI adoption

At a glance

What is changing:

AI optimism is growing as pilot projects switch to broader deployment

Why it matters:

Risk increases as AI use widens, amplifying any governance and control weaknesses

What to do:

Ensure AI risk is shared across functions, not loaded onto tech teams alone

AI optimism is booming. However, this may be blinding business leaders to the potential risks that are amplified when AI systems become embedded across an organisation.

A more balanced approach is needed.

"Organisations that treat AI as a pure opportunity are naive, and those that treat it as a pure risk will at some point be outpaced or outcompeted," says Gett's Matteo De Renzi.

With pilot projects moving to more structured deployment, a widening gulf is emerging between those who view AI as an opportunity and those who are proceeding with greater caution.

The risk concerns are not about the technology itself but the operational impacts that could expose existing weaknesses, with the rush to integrate AI potentially masking a growing governance gap.

"If you're going to use AI, the key lesson you need to learn beforehand is that your data has to be in really good shape," says IT consultant John Messina.

This matters because if data ownership is unclear or quality controls are weak, AI is likely to magnify those flaws.

"As I see it, AI doesn't correct those issues. Instead, it embeds them into automated decisions, often at scale, making problems harder to detect and unwind once they're in production," says Karen Schuler, Principal & Cyber Market Leader at BDO USA and Global Privacy, Data & AI Leader. "If your house wasn't in order, it's just going to get worse and be amplified after you implement AI.

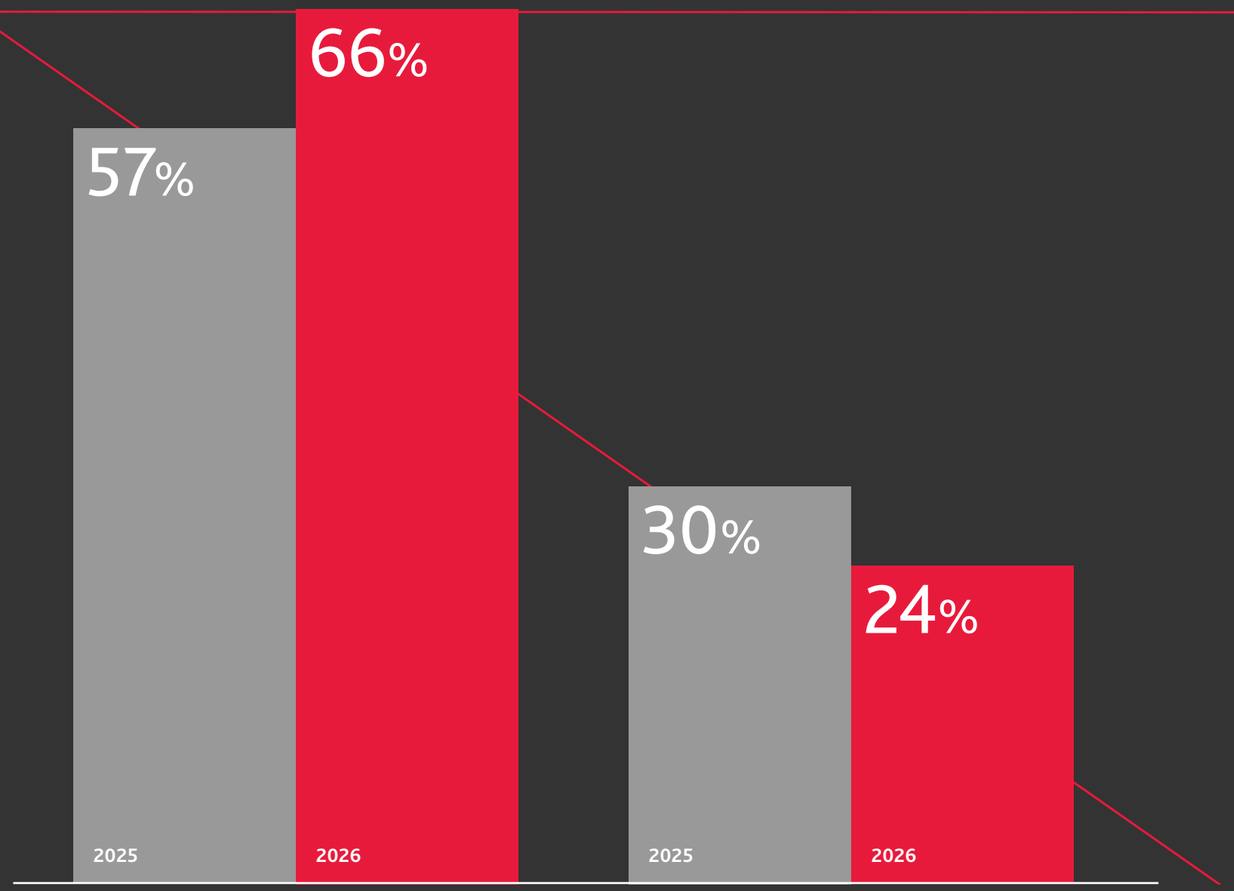
"From my perspective, since AI cuts across functions, it is essentially a stress test for organisational capability, revealing whether governance and controls are truly embedded and consistently applied."

Schuler contends a clearly defined risk appetite allows organisations to set the parameters for this stress test in advance, rather than discovering their limits only when something goes wrong. "These gaps aren't new, they've been around for a long time. But AI makes them more visible and more consequential," she adds.

That cross-functional impact also means AI risk accountability, in her view, needs to be shared across the business and not just left to technology teams.

> "AI is a stress test for organisational capability, revealing whether governance and controls are truly embedded and consistently applied."

AI confidence is rising as use cases become concrete



Schuler points out, "Organisations need to build a shared understanding of how to manage AI risk at scale. Not everybody has to be a data scientist, but it does require a baseline level of AI literacy across leadership teams so they can push that understanding down to their teams."

To improve organisational capability, business leaders must have the right risk culture in place. They also need a willingness to embrace organisational change.

Almost one in nine CEOs in the 1,500 largest publicly traded companies were replaced last year, the most since at least 2010, according to the Wall Street Journal.[2] This churn is a signal that old ways of thinking can no longer cut it in this new operating environment.

"Leaders who are set in their ways and resistant to change are not going to be the answer to where the business needs to go," says Ric Opal, Principal & National Leader, Cyber, IT Solutions at BDO USA and Global Digital Leader.

To navigate this, businesses should adopt a 'build, secure and grow' framework to AI that can help improve agility in uncertainty, ultimately enhancing business resilience.

The main AI risks sit in data, compliance and integration
The top five risks of AI that business leaders are most wary of

#1 | Data privacy

#2 | Compliance challenges

#3 | Cybersecurity

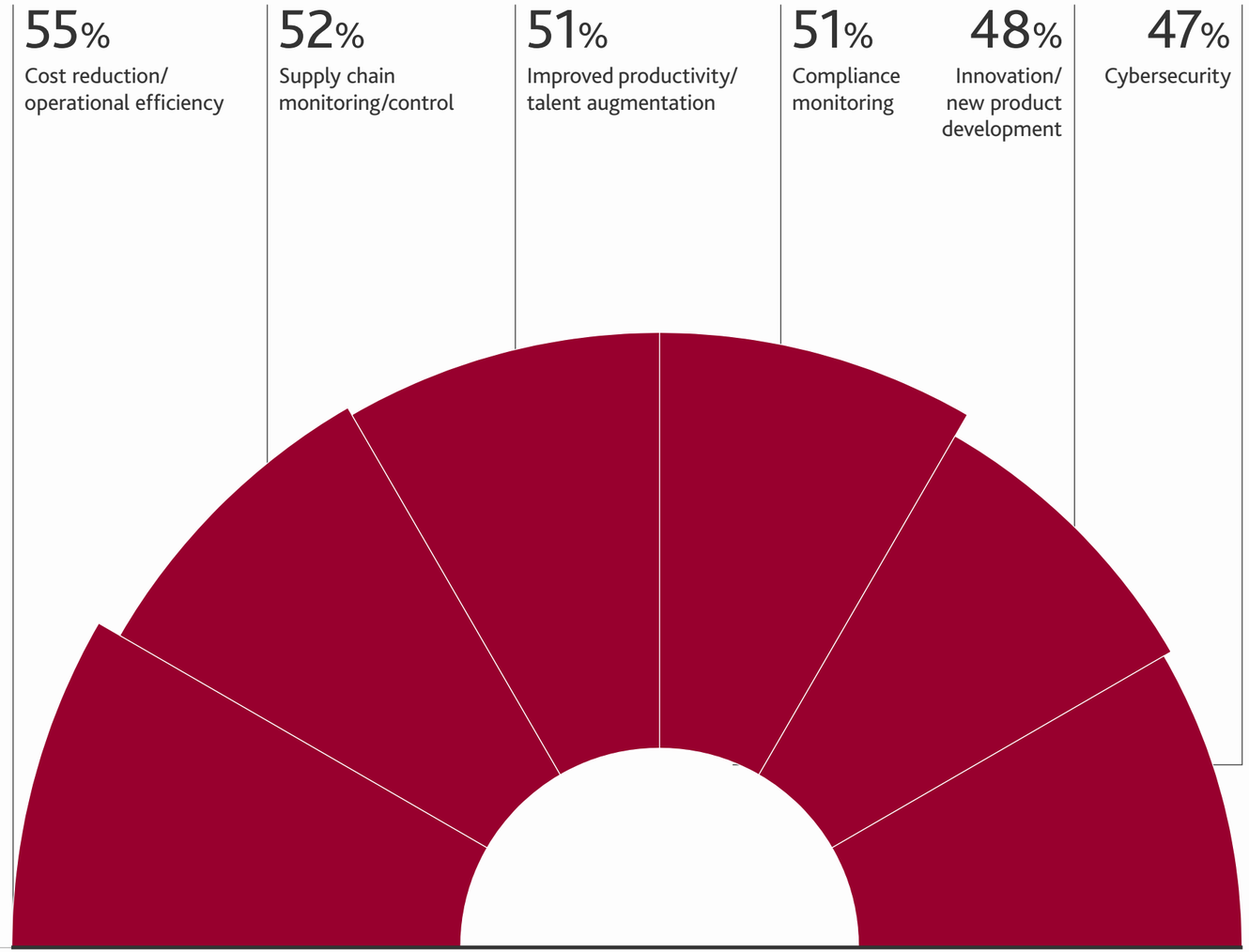
#4 | Integration challenges

#5 | Inaccurate predictions

Our 2025 Techtonic States report found that, by 2028, 62% of leaders expect AI adoption to be widespread across all areas of their business. Putting the right governance, controls and resilience in place will be key for organisations to scale their AI adoption with confidence.

"If you are resilient, you should be in a better risk position," adds Opal.

AI value is being captured inside the operating model first
Where AI is expected to have significant impact in the next year



2. Companies Are Replacing CEOs in Record Numbers—and They're Getting Younger

AI risk is evolving faster than businesses can keep pace

Karen Schuler
Principal & Cyber Market Leader at BDO USA and Global Privacy, Data & AI Leader

How AI adoption is outrunning organisational readiness

When emerging technology hits the market, businesses tend to adopt it and think about risk after the fact. This means risk is evolving faster than leaders fully appreciate, while adoption is accelerating more quickly than governance and organisational readiness. Leaders are focused on the upside: efficiency, speed, competitive advantage. But they're underestimating how rapidly risk profiles change once AI moves from pilot into live operations. That transition from experimentation to embedded use is an inflection point where risk becomes systemic rather than isolated.

Ric Opal,
Principal & National Leader, Cyber, IT Solutions at BDO USA and Global Digital Leader

AI misuse deserves as much attention as AI opportunity

There's also a broader lack of understanding of AI in business. As much as you might plan to use AI to grow faster and be more profitable, someone else will use it against you. The risks around AI's speed and sophistication are not yet well enough understood.

Ushering in risk management that acts, not reacts

Business leaders understand they can no longer just wait for stability to return. Uncertainty is the new norm and old ways of managing risk are becoming increasingly obsolete.

It is only by embedding risk management into operational processes across functions that organisations can enhance risk awareness, while also getting a clearer understanding of their overall risk position. This helps organisations remain agile enough to take calculated risks at the right time, ensuring business leaders can act decisively even in an era of heightened uncertainty.

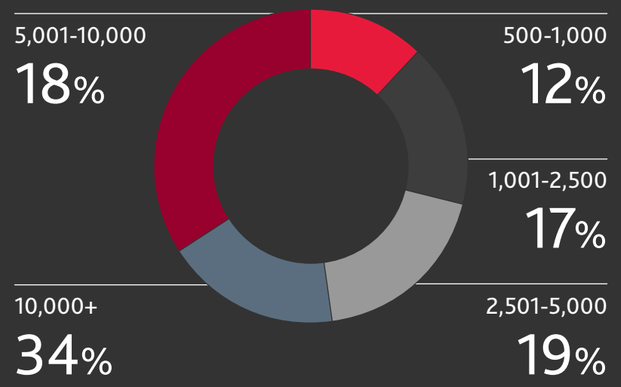
But agility requires clarity. Organisations that define their risk appetite upfront are better positioned to distinguish between risks worth taking and those requiring mitigation, rather than defaulting to blanket caution.

This approach is effectively a new operating model, where risk is not an enemy to be avoided but a commercial enabler that can be turned into a competitive advantage.

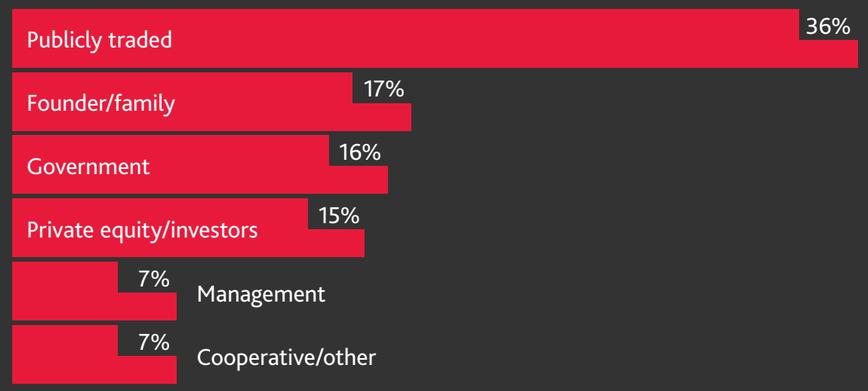
Methodology and demographics

BDO and alan. agency surveyed 500 senior executives (including CEOs, CFOs, CROs and CTOs) at businesses across a range of industries worldwide, including financial services, power and utilities, healthcare and life sciences, manufacturing, private equity and more. All businesses employed at least 500 staff and generated at least $100 million in annual revenue. The fieldwork took place between December 2025 and January 2026.

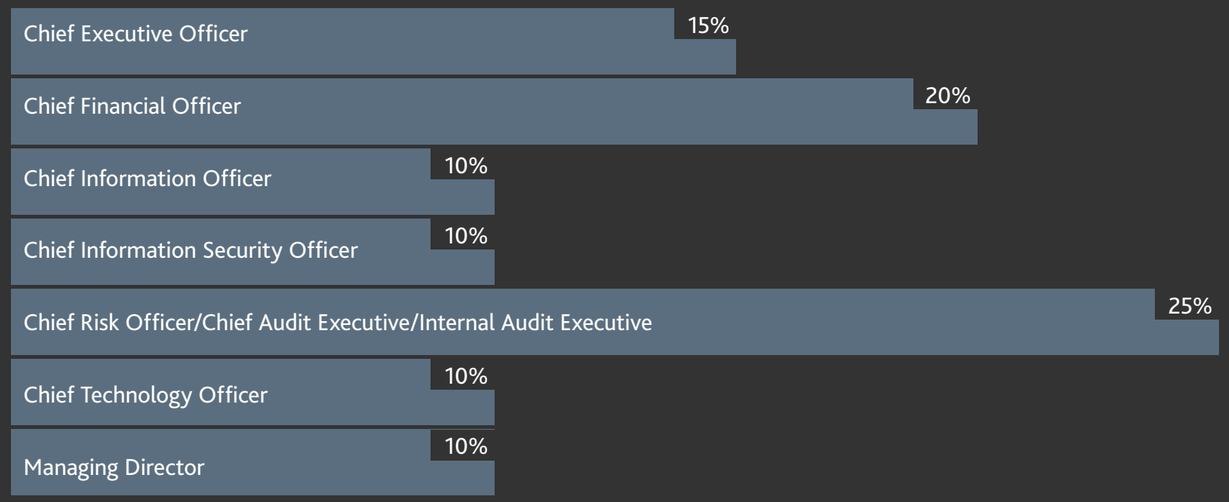
Employees



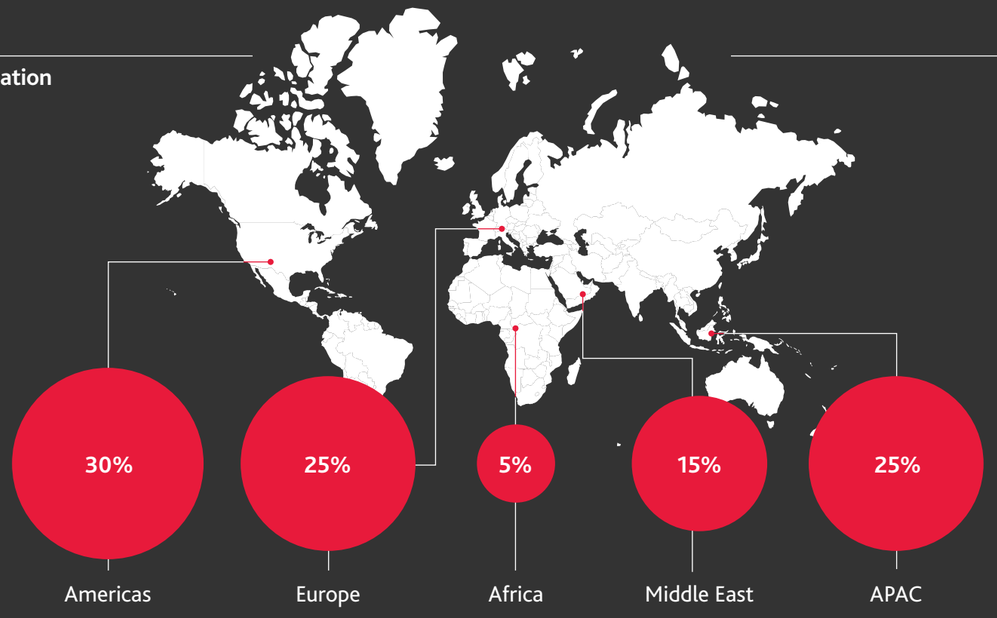
Company ownership



Job title



Location



Contributors

BDO contributors

Koen Claessens
Global Head of
BDO Risk Advisory

Alisa Voznaya
Partner and Head of Risk
Consulting at BDO UK

Ricky Cheng
Director and Head of Risk
Advisory at BDO Hong Kong

Richard Walker
Head of Risk Advisory Services
at BDO South Africa

Gonzalo García-Liñán
Risk Advisory Services
Partner at BDO Spain

Ziad Akkaoui
Partner and National Risk
Advisory Practice Leader
at BDO Canada

Erin Sells
Principal, Risk Advisory
Services at BDO USA

Rocco Galletto
Partner and Global Cybersecurity
Leader at BDO Canada

Glenn Pomerantz
Principal & Forensic Market
Leader at BDO USA

Markus Brinkmann
Partner and Head of Forensic,
Risk & Compliance
at BDO Germany

Karen Schuler
Principal & Cyber Market Leader
at BDO USA and Global Privacy,
Data & AI Leader

Ric Opal
Principal & National Leader,
Cyber, IT Solutions at BDO USA
and Global Digital Leader

External contributors

Matteo De Renzi
CEO at Gett

Johanna Pudda
CEO at Staci Americas

Richard Liao
CEO at Hwa-Hsia Glass

John Messina
IT consultant and former
CIO of the Canadian
government

FOR MORE INFORMATION

GONZALO GARCÍA-LIÑÁN
Partner, Head of Risk Advisory Services,
BDO Spain

gonzalo.garcia-linan@bdo.es

This publication has been carefully prepared, but it has been written in general terms and should be seen as containing broad statements only. This publication should not be used or relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained in this publication. No entity of the BDO network, its partners, employees and agents accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

'BDO', 'we', 'us', and 'our' refer to one or more of BDO International Limited, its network of independent member firms ('the BDO network'), and their related entities.

The BDO network (referred to as the 'BDO network') is an international network of independent public accounting, tax and advisory firms which are members of BDO

International Limited and perform professional services under the name and style of BDO (hereafter: 'BDO member firms'). BDO International Limited is a UK company limited by guarantee. It is the governing entity of the BDO network.

Service provision within the BDO network is coordinated by Brussels Worldwide Services BV, a limited liability company incorporated in Belgium.

Each of BDO International Limited, Brussels Worldwide Services BV and the BDO member firms is a separate legal entity and has no liability for another entity's acts or omissions. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, Brussels Worldwide Services BV and/or the BDO member firms. Neither BDO International Limited nor any other central entities of the BDO network provide services to clients.

BDO is the brand name for the BDO network and for each of the BDO member firms.

© Brussels Worldwide Services BV May 2026

www.bdo.global