Global Risk Landscape 2025

The Risk Rift: Why playing safe means losing growth

Foreword

In fast-changing times, proactive risk management is the key to growth

Ramsés Inzunza Espinosa
Risk Advisory Partner,
BDO Mexico

ramses.inzunza@bdomexico.com

The lesson from the past 12 months is clear: forget about waiting for the turbulence to pass. In an era of non-stop crisis, businesses that want to grow and meet their targets must take a proactive approach to risk.

The problem is that few are - and things are getting worse. This is our 10th annual report on global risk, and it is remarkable that our survey of 500 senior leaders worldwide found that 69% now say their companies are risk-averse or risk-minimising, compared to 61% last year. This is likely to have grown even more since we conducted the survey, given the increasing risk of a global trade war and frequent US policy changes.

Senior managers were already frustrated with their risk management efforts. Given a list of six risk management failings, executives on average said half applied to their organisation. None of the 500 global respondents, all senior leaders, gave their risk management a clean bill of health. Notably, CEOs were particularly critical of compliance overspend, suggesting that risk management strategies as they stand are failing to deliver value.

Part of the problem is that businesses are increasingly taking a compliance-led approach to risk, with a box-ticking mentality distracting from real risk management.

Fortunately, many executives recognise this as an issue – 74% say that embedding risk thinking in the company culture will start to tilt the balance from a heavy focus on compliance to real risk strategies that can deliver more value and opportunities for the business.

This means recognising that growth will require change, which also means that the risk landscape will shift, potentially exposing the business to additional risk vectors in areas such as supply chain or cybersecurity.

It has never been more critical for businesses to take a proactive approach to risk and ensure their risk management strategies are not weighed down by box-ticking. If they can make this adjustment, businesses can improve their risk posture and ensure they are better placed to take advantage of the many opportunities the current global risk landscape is creating. ■

69% of companies say they are risk-averse or risk-minimising against...

61% in 2024

74% of executives say embedding risk thinking into their business culture is a priority

Contents

Executive summary

On a cliff edge: the state of risk in 2025

Some 84% of executives say the global risk landscape is more than ever defined by crisis. As a result, many businesses are taking a safety-first approach – but this risks sacrificing growth.

See page 06

THE TOP RISKS ORGANISATIONS ARE UNPREPARED FOR

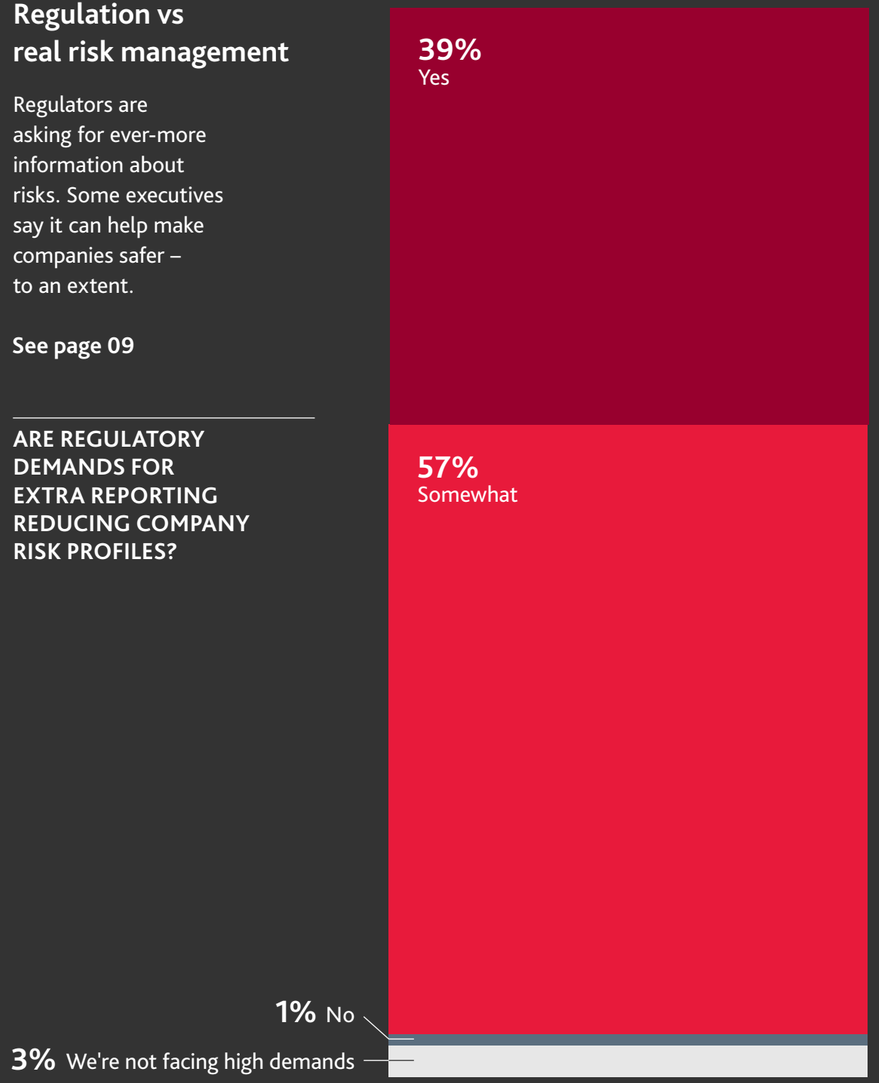
Rank	Risk Area	Position Change	
1	Regulatory risk	▶ Same as 2024	35%
=2	Supply chain	▶ Same as 2024	28%
=2	Talent or people	▲ 10 places	28%
4	Geopolitical tensions	▶ Same as 2024	25%
5	Environmental	▲ 4 places	24%
6	Cybercrime	▼ 1 place	23%

Regulation vs real risk management

Regulators are asking for ever-more information about risks. Some executives say it can help make companies safer – to an extent.

See page 09

ARE REGULATORY DEMANDS FOR EXTRA REPORTING REDUCING COMPANY RISK PROFILES?

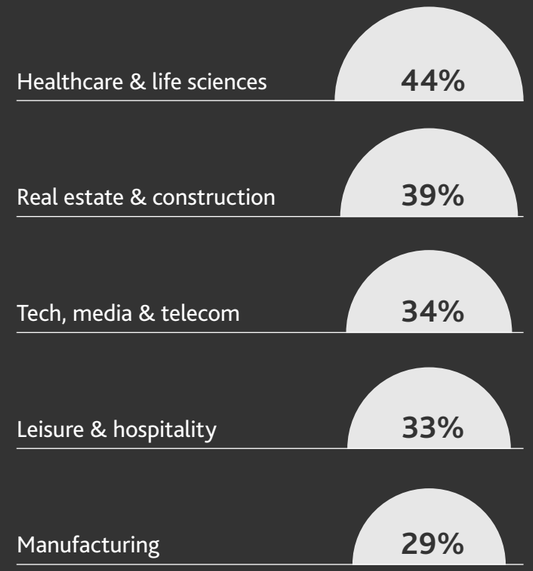


Workforce risk is back on the agenda

For the first time since the pandemic, companies are getting worried about talent and people risks – 28% said one of these was a top three risk, against just 12% in 2024. AI could make this issue more pressing.

See page 11

THE SECTORS WHERE LEADERS ARE MOST UNPREPARED FOR PEOPLE/TALENT RISK



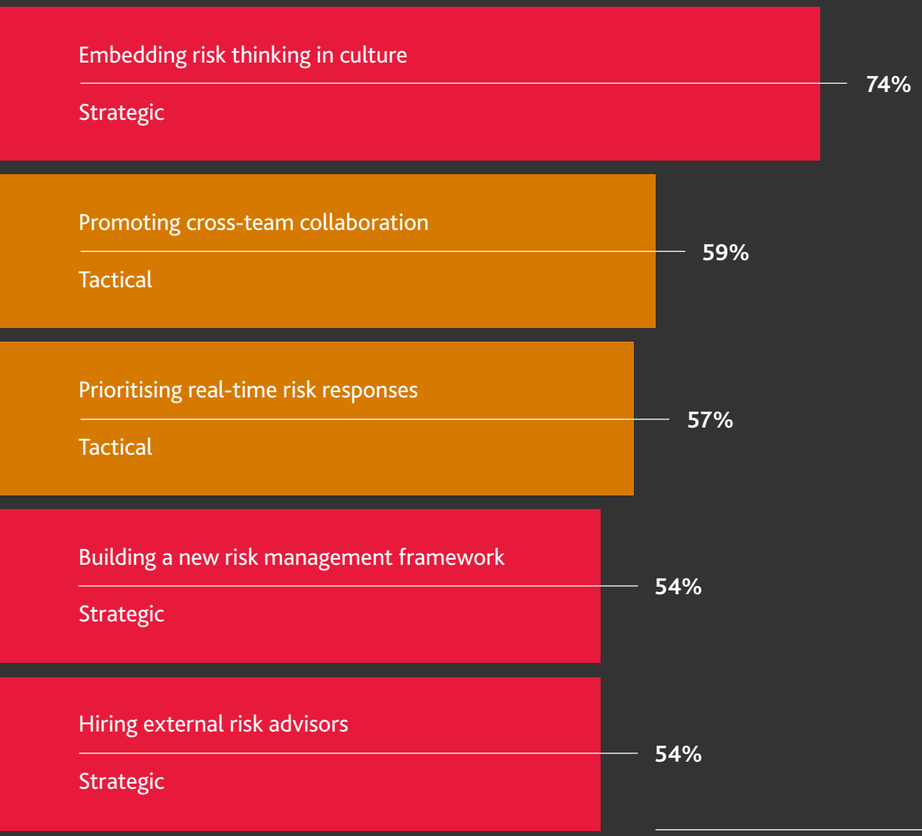
Survey of 500 C-suite executives worldwide conducted for BDO in January 2025. Full survey details on page 30.

The risk rift

Regulators' demands for information on risk can help drive risk reduction – up to a point. Companies must not create a box-ticking environment that can distract from real risk management strategies.

See page 12

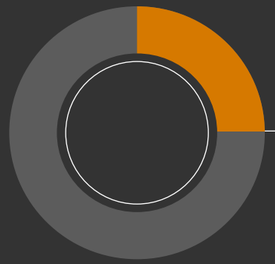
WHAT ARE COMPANIES DOING TO TILT THE BALANCE TOWARD REAL RISK MANAGEMENT?



Cyber breaches: no end in sight

Cyberattacks are rising up the risk agenda as the threat landscape continues to evolve, accelerated by AI. However, CTOs are worried that the growing focus on cyber compliance might distract from practical risk reduction.

See page 16



25%

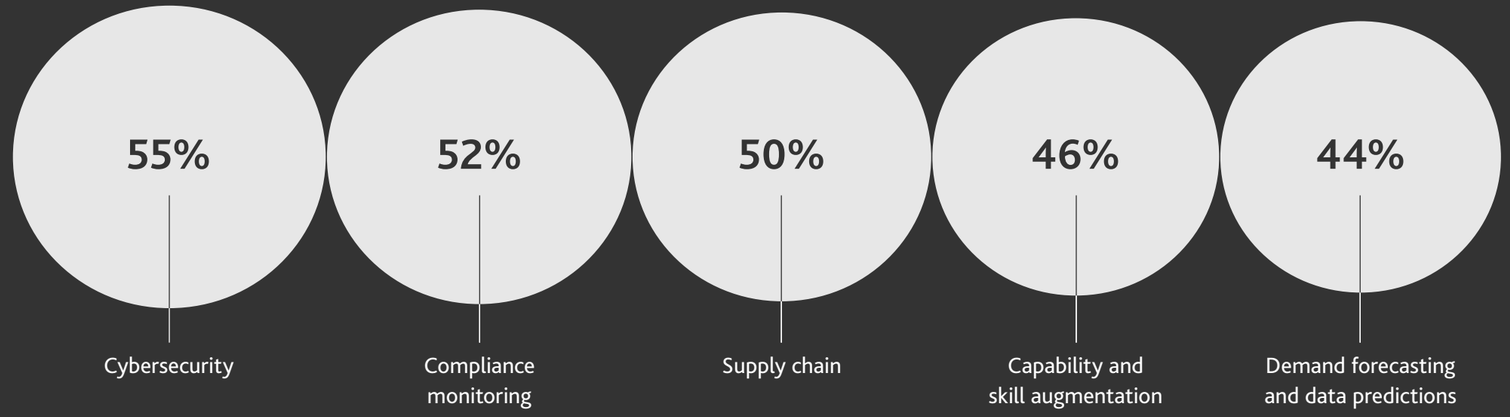
of CEOs cite cybercrime as a top three risk in 2025

The risk/reward gap on AI

Attitudes towards AI have shifted again over the past year – more executives see it as an opportunity than a risk (but some see it as both). Leaders believe AI can improve risk management, but a thoughtful, structured approach is needed.

See page 21

WHERE AI IS EXPECTED TO HAVE THE MOST IMPACT IN THE NEXT 12 MONTHS

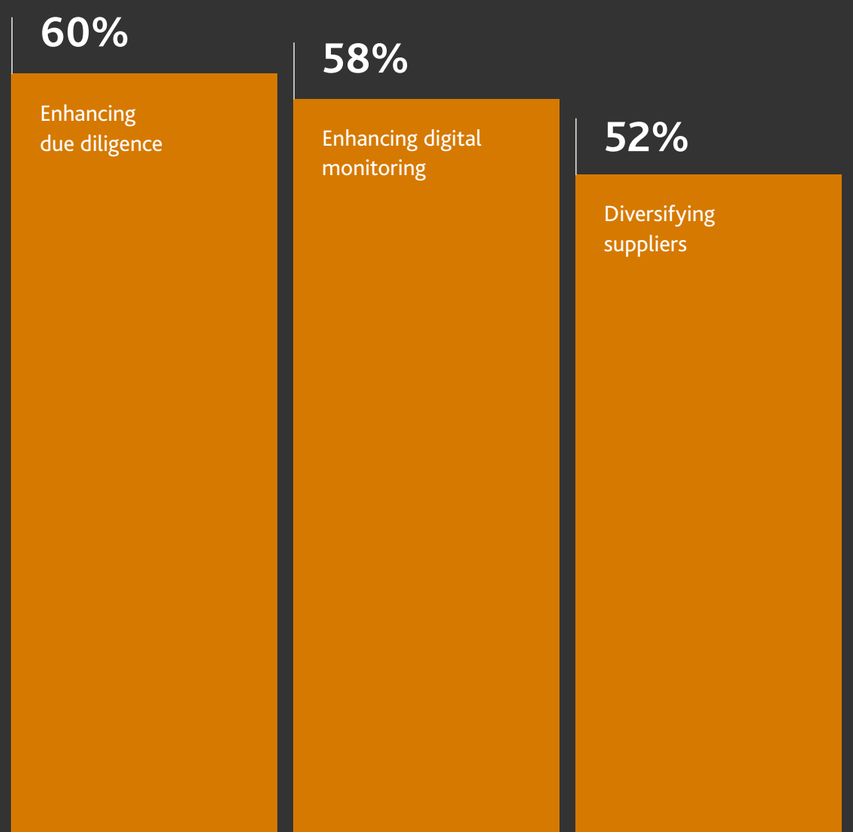


Avoid supply chain ruptures by 'flexsourcing'

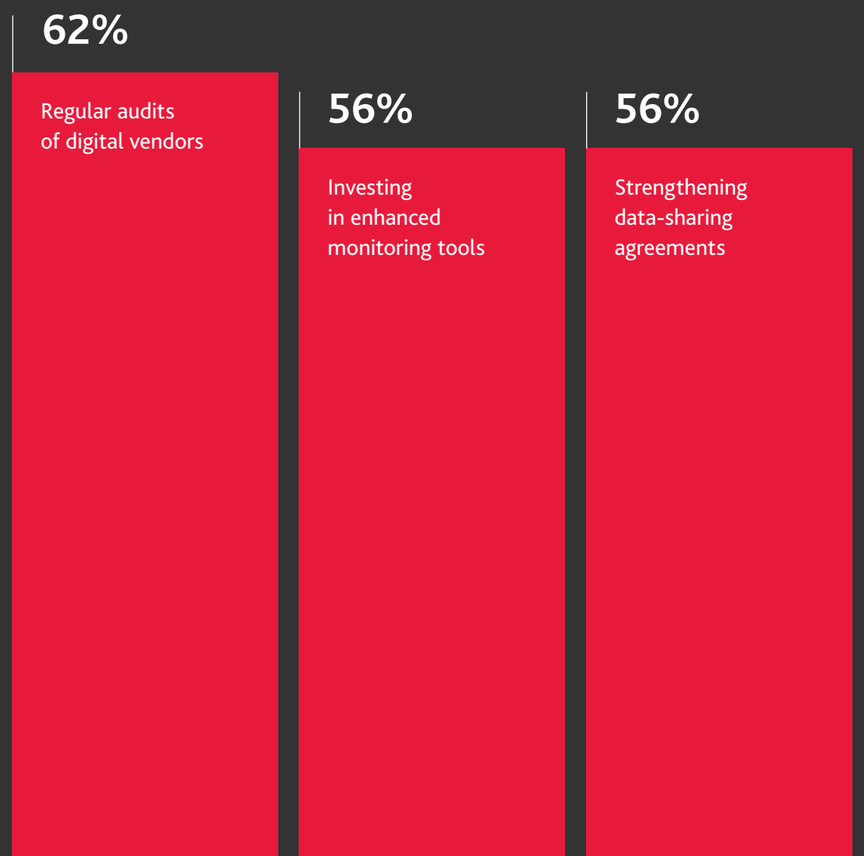
Supply chains are under strain, with the threat of tariffs and the need to switch sources likely to make things worse. Firms need to consider 'flexsourcing', a hybrid approach that blends nearshoring with friendshoring, building the agility to switch procurement to countries with more reliability or lower tariffs.

See page 25

THE TOP THREE WAYS COMPANIES ARE STRENGTHENING THEIR PHYSICAL SUPPLY CHAINS



AND THE TOP THREE WAYS COMPANIES ARE STRENGTHENING THEIR DIGITAL SUPPLY CHAINS



Don't give fraudsters a chance

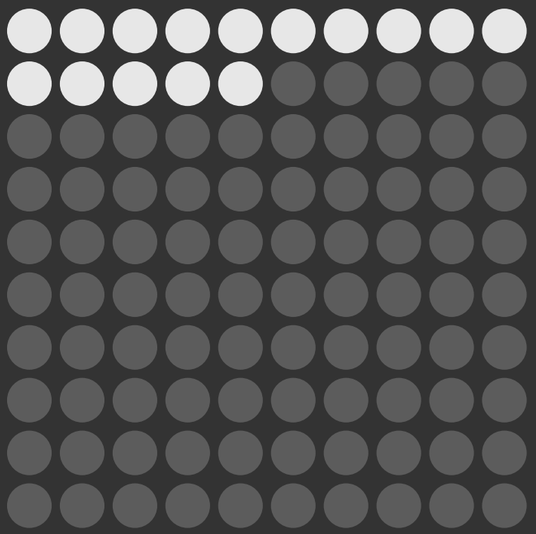
Fraud risk is underappreciated and sometimes misunderstood, with only 15% of executives citing it as a top three risk. As fraudsters exploit AI to find new vulnerabilities, it's time for companies to prioritise.

See page 27

Only

15%

of executives cite fraud risk as a top three risk



On a cliff edge: the state of risk in 2025

Organisations may stagnate if they don't proactively embrace risk

At a glance

What is changing

The global risk landscape faces greater uncertainty than ever, prompting companies to take a more defensive approach to risk management.

Why it matters

This 'wait and see' approach is not suitable for the 'permacrisis' era – it will limit growth opportunities and risks holding companies back.

What to do

While the timidity is understandable, businesses must take a proactive approach that weighs their risk appetite against what could go wrong, and plan accordingly.

From escalating world trade tensions to shifts in geopolitical relationships, the global risk landscape has been in flux for more than a decade – and shows no sign of stabilising. The perceived level of crisis among risk professionals and senior executives remains at record levels, with 84% of respondents in the survey saying the global risk landscape is more defined by crisis now than ever.

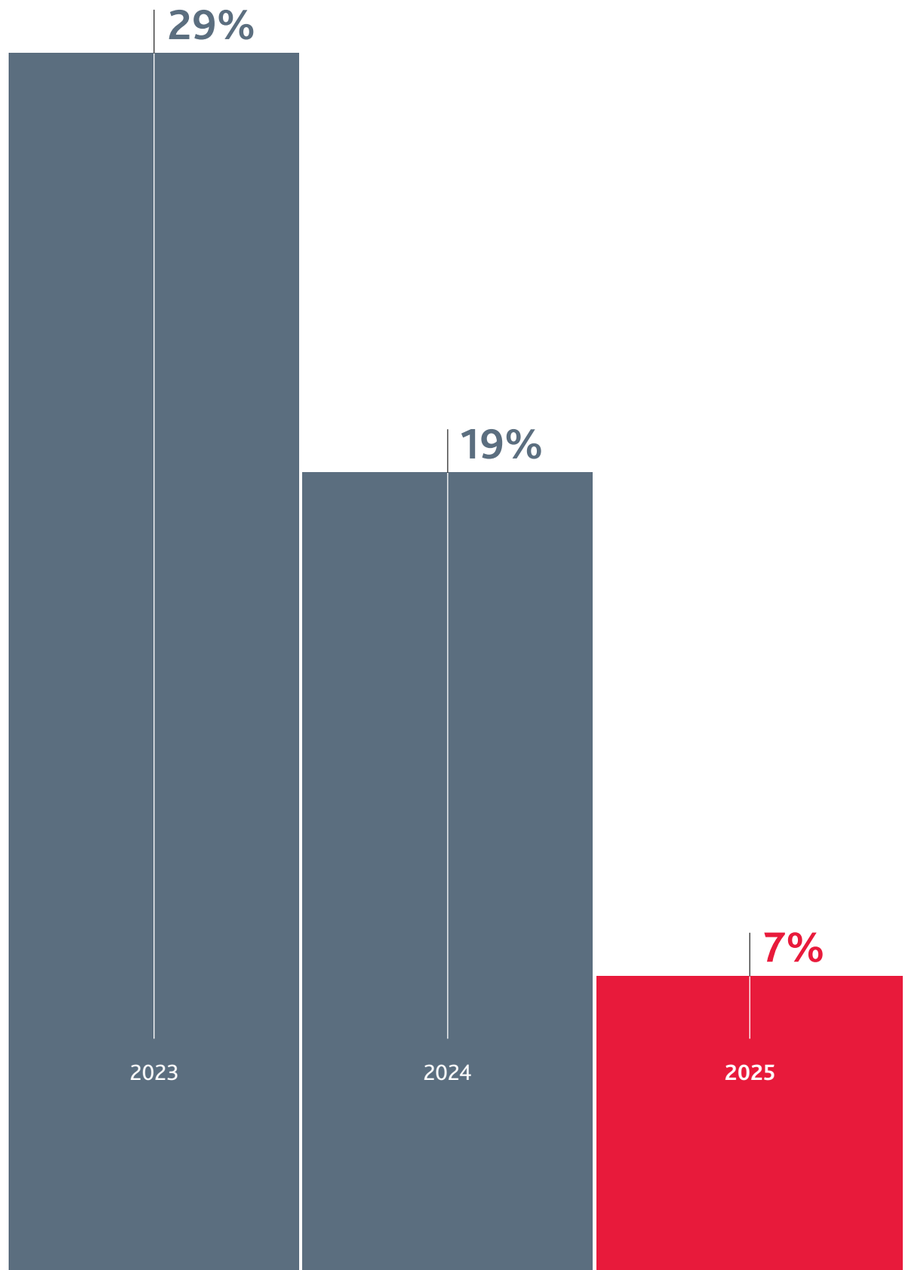
Against this backdrop, businesses are struggling to navigate a path forward.

Only 7% of executives said their risk management is 'very proactive', down from 19% in 2024 and 29% in 2023. This matters: if companies are overly cautious, it will weigh on growth and increase pressure from stakeholders. ▶

84% say the global risk landscape is more defined by crisis than ever

PROACTIVE RISK MANAGEMENT IS BECOMING RARE

Percentage who say their risk management is 'very proactive'



"The chaos and volatility that's all around us right now is definitely disrupting business," said Dave Arick, Managing Director for Global Risk Management at claims management and loss adjusting business Sedgwick. "You see a lot of hesitation from businesses as they look at investments and growth, because they don't know where the next curveball is going to come from, so there's a bit of a 'wait and see how it plays out' mentality."

The challenge with adopting this stance is that if the problems just keep mounting, businesses will stagnate.

"Waiting for it to settle down means you're going to end up with a lot of businesses being paralysed by fear of what could go wrong," Arick said. "There's a lot of reasons to be cautious, but you don't meet your targets by being cautious."

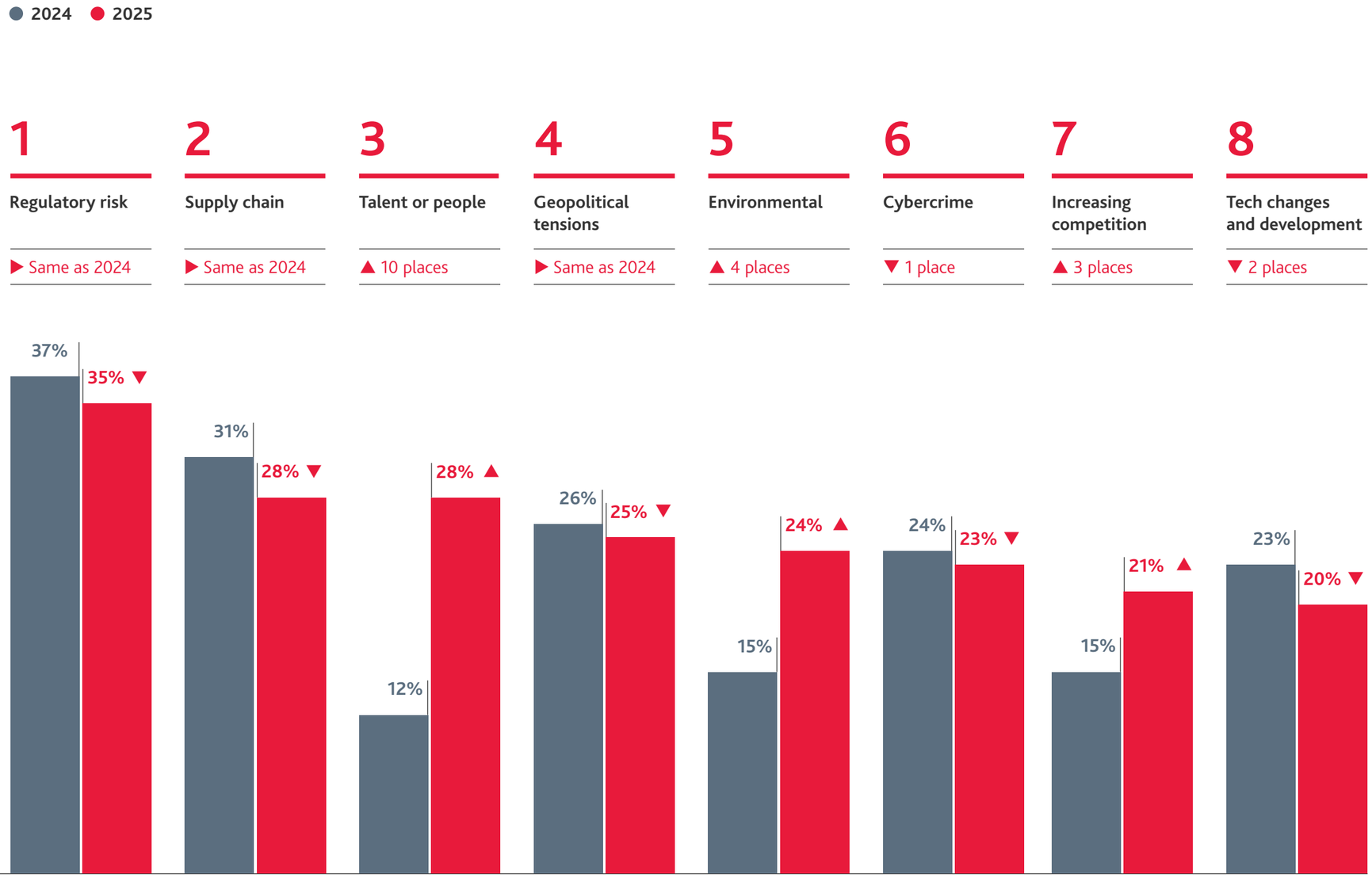
A better approach in this environment is to engage in scenario planning and anticipate the things that could go wrong so businesses can start to seize opportunities instead of sitting on their hands waiting for the turbulence to subside.

"Even for aggressive companies that want to take a big swing at something that's maybe transformative for that business, you can still put some planning in place to think through the potential things that could go wrong," said Arick. "How do we best prepare so that we're not caught flat-footed if those things do happen?"

Scenario planning is not just a one-and-done exercise given how fast the global risk landscape keeps changing. ▶

WHICH RISKS ARE ORGANISATIONS MOST UNPREPARED FOR?

Data shows the risks chosen among top three by respondents



"We're doing our goal-setting and strategy for the year and part of that process is to analyse and review the top risks for the moment, ensuring we have the right remediations in place," said Lianne Appelt, Head of Enterprise Risk Management at Salesforce. "The landscape has changed significantly since our last internal risk assessment back in December and the regulatory landscape I would say is the biggest change."

This increased regulatory burden may be prompting businesses to take a more 'safety first' compliance approach to risk management, which steers risk managers to be more reactive than proactive.

"The risk landscape is large and it is evolving rapidly, so it is difficult to keep up with all the things the companies are facing," said Dawn Williford, Principal, Risk Advisory Services at BDO USA. "However, in the long run, if you were actually spending the money up front to identify and manage risk versus reacting to it, the cost could be much less – that's the biggest benefit of having a proactive approach."

Regulatory risk remains the top risk among C-suite executives, with 35% selecting it as one of the top three risks they feel most unprepared for.

"Companies feel that regulation is a burden because the regulators are becoming less predictable," said Emanuel Van Zandvoort, Partner, Risk Advisory Services – Enterprise Risk Management at BDO Netherlands. "In Europe, companies have to invest a lot in compliance and then laws and regulations change overnight."

Some 52% of respondents named data privacy as one of the top three most important regulations for their business, more than any other type of regulation.

Supply chain risk and people/talent were joint second – a big jump for people risk which was only in 12th place in 2024 (see page 11). Geopolitics remains a concern, placed at fourth.

Geopolitics is also adding to the heightened sense of uncertainty globally, where businesses are dealing with confusion around tariffs and escalating trade tensions, which in turn is fuelling the 'wait and see' approach. The friction between the US and China is also adding pressure on businesses, particularly in the APAC region.

"The first thing is the Sino-US trade war, and the second thing is about the relationship between Taiwan, US and China, so the situation in the APAC region is quite tense," said Ricky Cheng, Director and Head of Risk Advisory at BDO Hong Kong.

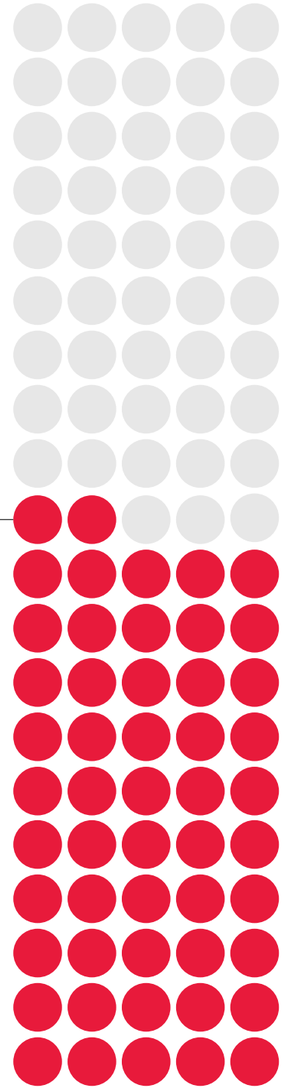
Environmental risk is another fast-rising issue, moving up four places to fifth, with 24% now saying they are unprepared for this. Cybercrime is still very much on the radar: it was ranked sixth. ■

> "Companies feel that regulation is a burden because the regulators are becoming less predictable."

Emanuel Van Zandvoort,
Partner, Risk Advisory Services –
Enterprise Risk Management, BDO Netherlands

52%

see data privacy as one of the three most important regulations for their business



Can regulation help shine a light on real risk management?

Reporting requirements may help focus minds on risk, but could create complacency

At a glance

What is changing

The regulatory burden on companies continues to grow, with compliance teams facing additional reporting requirements.

Why it matters

An increased focus on regulation can create a box-ticking environment that distracts from real risk management.

What to do

Regulation can feed into risk thinking but organisations must always focus on the macro and micro risks a business faces.

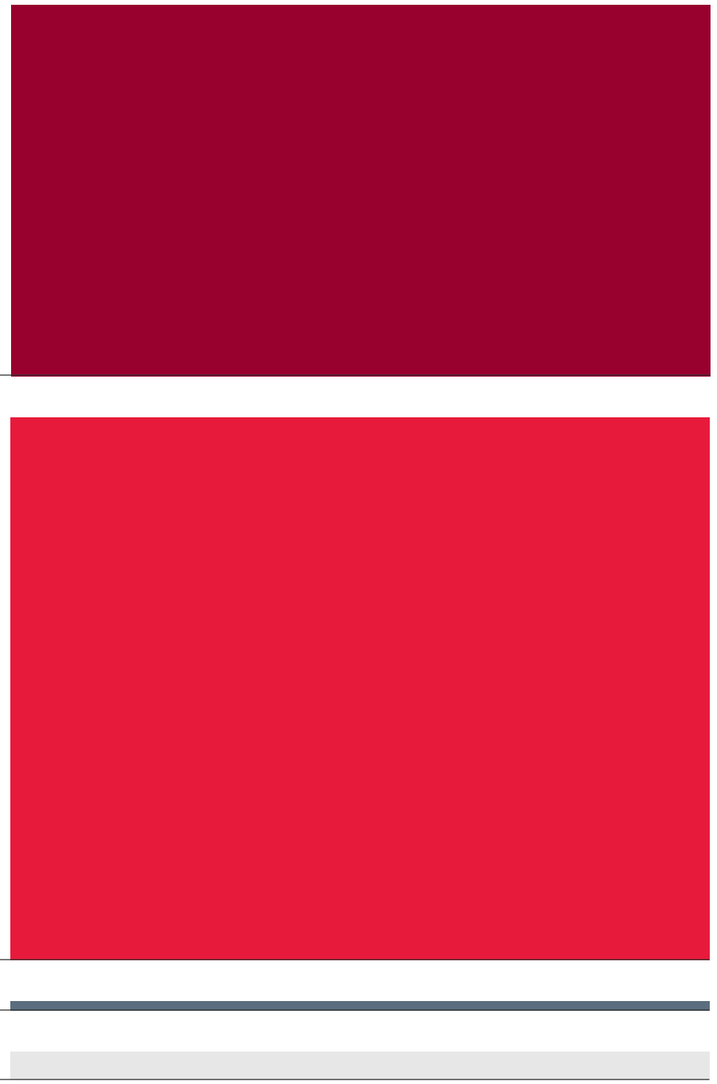
Businesses face increasing volumes of regulation, particularly those that operate across borders. While this adds to the compliance burden for risk managers, a majority of C-suite respondents said that regulators' demands for additional reporting were generally helpful in reducing their overall risk.

More than a third of respondents (39%) said that increased regulation reduces their risk profile, while another 57% said it somewhat reduced their risk.

However, it should only ever be viewed as one component of an organisation's risk management strategy.

"Regulation is one aspect of risk management, but I don't think regulation will give you a full picture of your risk environment. It can help, but you'd be missing the exercise if you take it from a compliance-first approach, as opposed to focusing in on the macro and micro events and threats that exist within a specific organisation," said Ziad Akkaoui, National Practice Leader, Risk Advisory at BDO Canada.

ARE REGULATORY DEMANDS FOR EXTRA REPORTING REDUCING COMPANY RISK PROFILES?

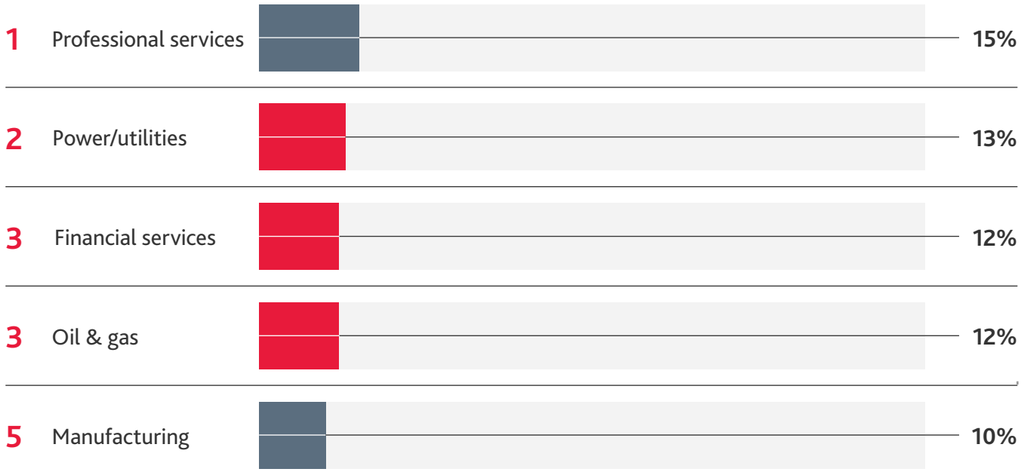


The potential for regulation to support more proactive risk management could hinge on the volume of regulation a business faces. Companies in industries that are heavily regulated said they are more likely to deal with risk very proactively, with power and utilities (13%) and financial services and oil and gas (both 12%) businesses taking steps to stay ahead of risk. This is likely because the pace of regulatory change means companies in these sectors have to constantly adjust to changing risk thresholds set not only by their boards but by the regulators too, said Enric Doménech, Head of Risk Advisory Services at BDO Spain.

While not a heavily regulated industry, 15% of professional services firms said they deal with risk very proactively. This is potentially not just because of regulatory concerns but also because a breach of client data could be reputationally fatal for a firm. ■

TOP FIVE SECTORS THAT SAY THEY DEAL WITH RISK 'VERY PROACTIVELY'

● **Heavily regulated industries**



People risk is climbing up the agenda again

Executives are increasingly worried about access to talent

The biggest change to the rankings for 2025 is the sharp increase in concern about people and talent. More than a quarter of executives (28%) said talent or people capacity is a top three risk, up from 12% in 2024. While 'people capacity' and 'talent' separately rank relatively low on the list of risks executives feel unprepared for, when combined they rank joint second – above longstanding problems such as geopolitical tensions and cybercrime.

Concerns vary by sector. Healthcare and life sciences are most concerned about people/talent (44%), followed by real estate and construction (39%), and then tech, media and telecom (34%).

"There is a scarcity of talent, and trying to retain good people and trying to attract really good people is hard," said Dave Arick, Managing Director for Global Risk Management at Sedgwick. "Being able to speak the language of risk is something that is really important for all of us in the world that we're in today."

"Just finding the right people to add to your workforce that can have their eyes and ears open – even if their day job isn't risk management – is getting harder. My view is that we're all risk managers to some degree."

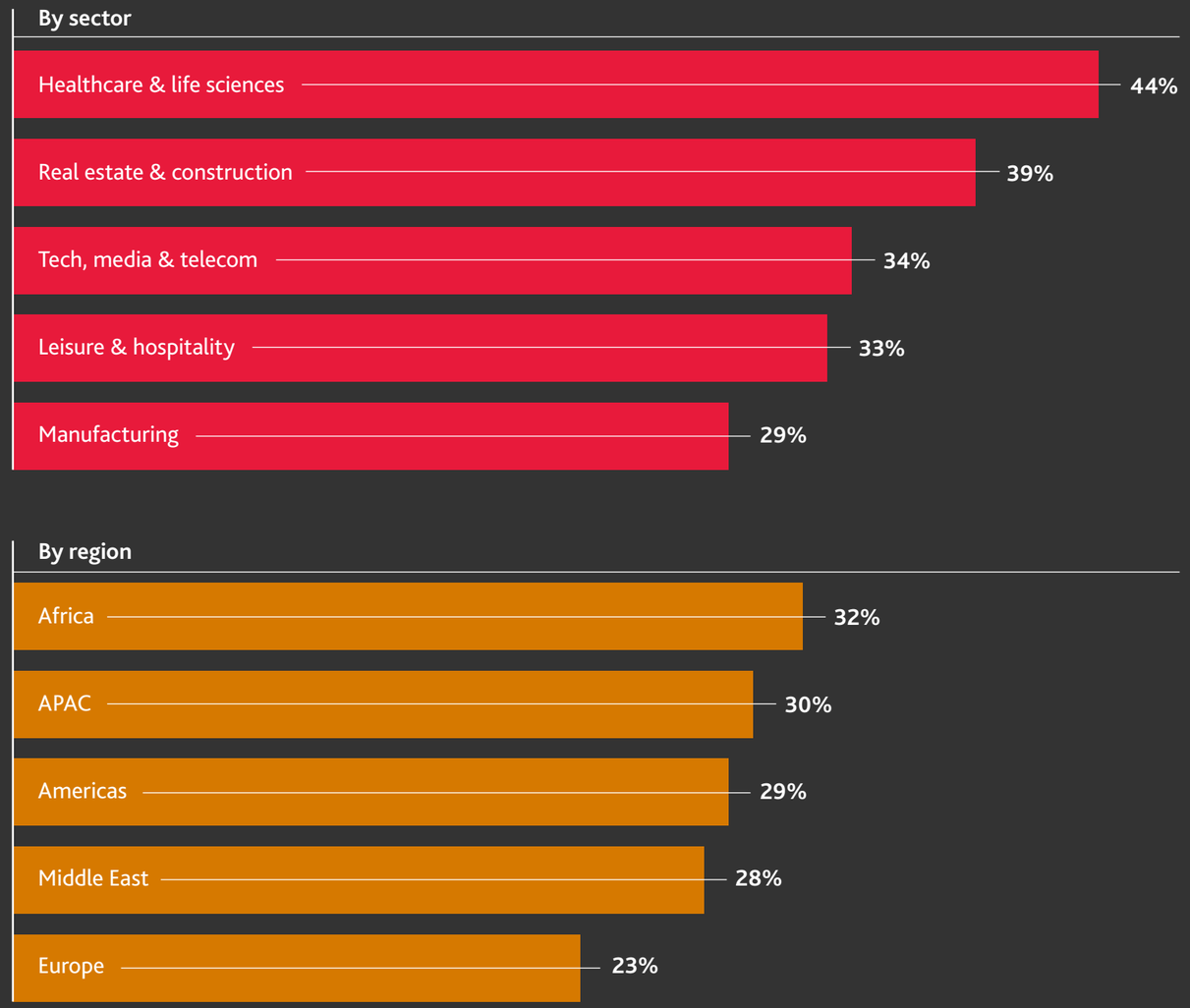
AI may also be impacting perceptions of people risk, not just because businesses will increasingly need talent who are proficient in AI – either as users or developers – but because the rise of the technology may chip away at institutional knowledge and have a long-term impact on training and employee skills.

"Manual tasks are being stripped out, but that's how people learn when they come into risk," said Alisa Voznaya, a Partner leading BDO's Consulting practice in London. "You need people to understand what actually happens in the weeds. When you strip that out, you lose the opportunity to train people with that view. So there is a concern about how you get that experience – we don't want to lose that muscle memory."

28% said talent/people capacity is a top three risk they are unprepared for against

12% in 2024

WHERE IS TALENT/PEOPLE RISK HITTING HARDEST?



The risk rift: how a compliance-led approach is holding back growth

A focus on box-ticking may be overshadowing real risk management strategies

At a glance

What is changing

Increased regulation and an uncertain operating environment are prompting businesses to take a more compliance-led approach to risk management.

Why it matters

This approach often takes precedence over real risk management, which means businesses may be missing out on or overlooking potential growth opportunities.

What to do

Embedding a risk culture helps shift the mindset away from a compliance-led approach and instead embraces risk to identify growth-driving business opportunities.

Executives think they have the right balance between real risk management – the broad risks that are a potential threat to a company – and compliance. But take a closer look at those assertions and it reveals potential fractures inside the organisation.

While a majority of respondents say there is an equal focus between risk and compliance (54%), the survey shows that CEOs/MDs are not on the same page as their Chief Risk Officers (CROs). Company leaders say their biggest problem is compliance overspend, followed by a box-ticking mentality. By contrast, CROs say their biggest problem is limited adaptability to new risks, followed by minimal use of monitoring tech.

The regulatory backdrop may also be forcing companies to take a more compliance-led approach given that broad market uncertainty introduces even more unknowns into risk-taking.

"The regulatory environment is seeing sudden shifts and downright reversals rather than a gradual drift under the current administration," said Polly James, Senior Director of Risk Management at Feld Entertainment in the US. "A rush to reduce federal ▶

oversight and push regulation down to the state level is not helpful for businesses that operate across the country."

Getting the balance right between real risk management and compliance is essential if companies want to be more proactive around risk.

"Regulatory and compliance risks have always been at the forefront of our risk landscape, but what is happening this year is unique. It's important to really stay on top of it, because that enables us to not really have to stop or pause other activities or innovations in pursuit of compliance activities," said Lianne Appelt, Head of Enterprise Risk Management at Salesforce.

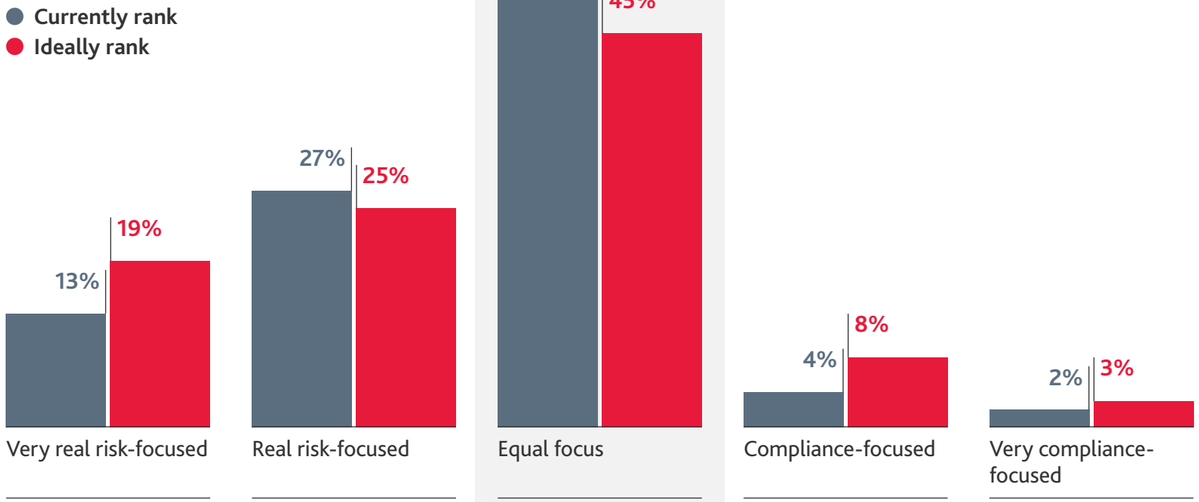
Most businesses recognise the need to increasingly focus on real risks. As many as 74% of executives said it is a priority to embed risk thinking into their company culture.

"There definitely needs to be awareness of what risk means for individuals and the business, as well as the upside of operating with a mindset that is aligned to a company's strategic objectives and values." said Matt Williams, a Partner in BDO Australia's Risk Advisory Services team.

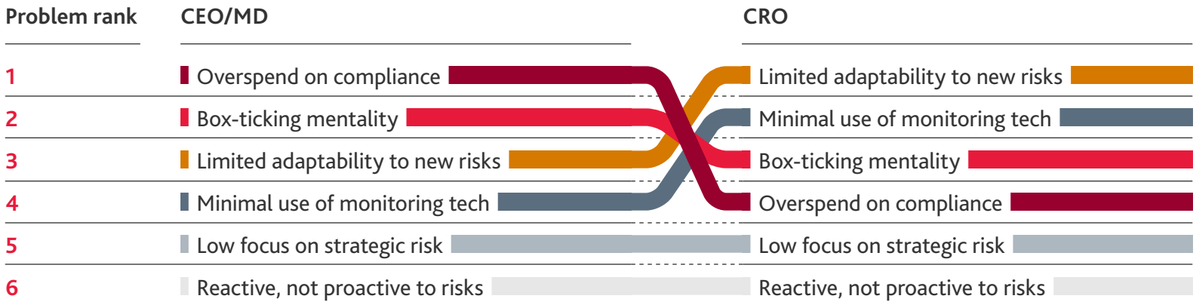
Another issue is the apparently contradictory views of senior leadership. While 63% of CEOs and managing directors said regulatory risk is one of the top three risks they are unprepared for, 60% also said that compliance overspend is a major problem.

One potential reason for this mismatch is that business leaders think their companies are not getting the best value out of their compliance and regulation efforts because they are too focused on box-ticking rather than finding ways to capitalise on their risk management. ▶

REAL RISK VS COMPLIANCE FOCUS: EXECUTIVES SEEM COMFORTABLE IN THE MIDDLE



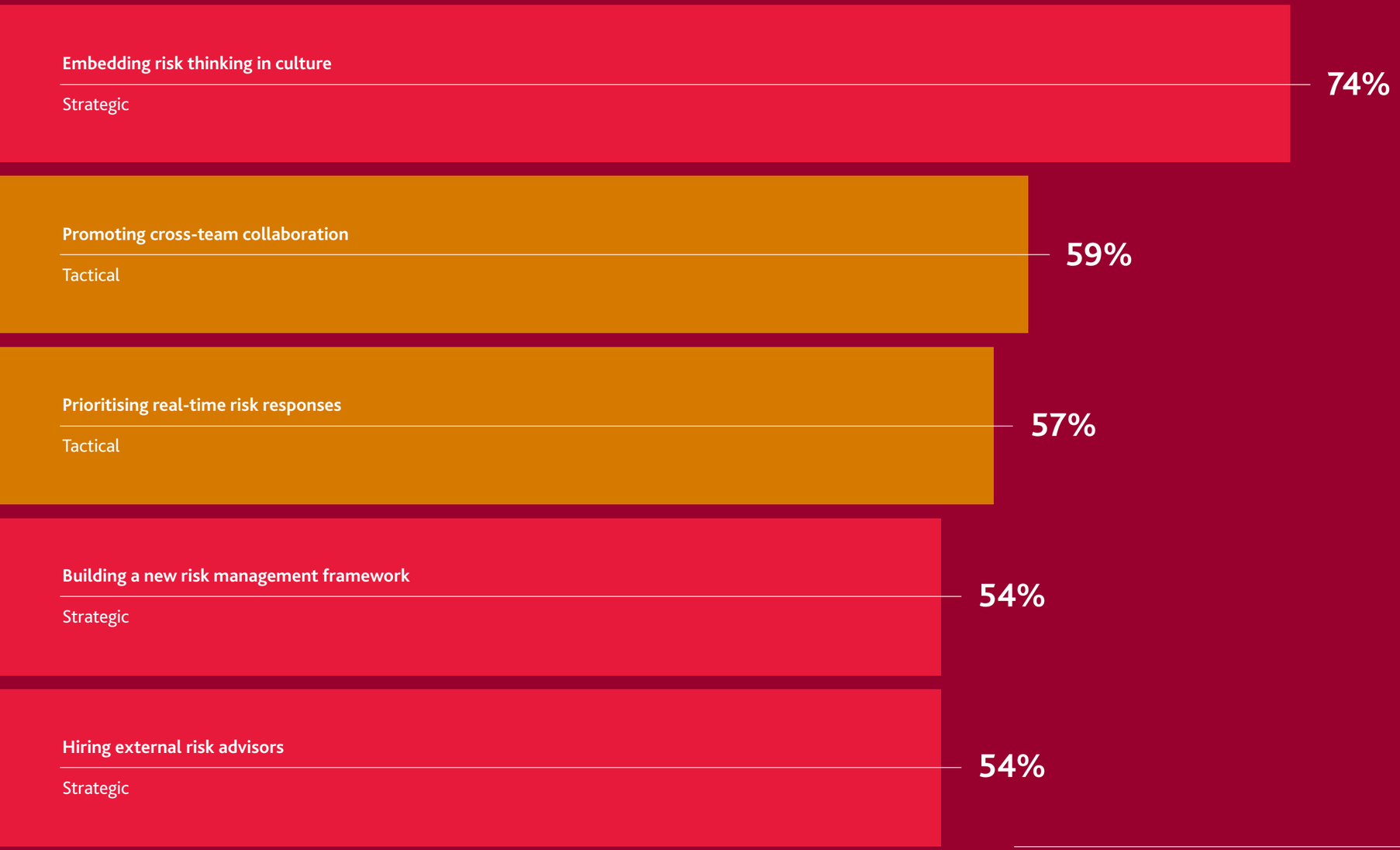
BUT LOOK DEEPER – CEOs/MDs ARE HIGHLY CRITICAL (AND THEY DON'T ALIGN WITH THEIR CHIEF RISK OFFICERS)



> "Regulatory and compliance risks have always been at the forefront of our risk landscape, but what is happening this year is unique."

Lianne Appelt,
Head of Enterprise Risk Management,
Salesforce

WHAT ARE COMPANIES DOING TO TILT THE BALANCE TOWARD REAL RISK MANAGEMENT?



While some CEOs might complain that compliance is too expensive because it doesn't contribute to their bottom line, 'underspending' could potentially have damaging consequences, said Richard Walker, Head of Risk Advisory Services at BDO South Africa.

"Businesses must weigh the risks and opportunities: while saving on compliance overspend is tempting, getting caught can result in hefty fines and damage to reputation," said Walker.

Some businesses are investing in risk in other ways, for instance by hiring consultants. However, appetite for this approach often depends on a business's ownership structure. For example, 67% of management and PE-owned businesses said they are engaging consultants to ensure a focus on real risk management, though founder-owned companies were less likely to do this (just 43%).

Insight

Say goodbye to box-ticking

Alisa Voznaya
Partner leading BDO's Consulting practice in London

"Organisations sometimes feel that a compliance approach is easier – you follow the processes and you feel like you've done your job, you feel good about yourself. You get a dopamine rush. Whereas with a risk culture, it almost feels like the hardest thing to possibly do.

Organisations need to recognise this and ask themselves, do we talk about risk strategically or do we talk about risk as a tick-box exercise? The telltale sign for me is how much time is spent by functions focusing on the compliance elements that need to be filled in, without ever really bringing those risk assessment conversations to the executives. This means executives are not considering these issues as part of their agenda.

There can also sometimes be a lack of understanding on how the compliance programme connects to risk. In those situations where you have compliance and risk functioning independently – unless it's obviously a very regulated environment – that's problematic because ultimately they're driving towards the same purpose and just looking at it through a different lens." ■

Cyber breaches: no end in sight

The evolving cybercrime threat is keeping executives on their toes

At a glance

What is changing

Cybercriminals are getting ever more sophisticated, which is making CEOs sit up and take notice, particularly if competitors have been impacted.

Why it matters

Cyberattacks can cause severe reputational damage and result in significant regulatory penalties for companies who don't take adequate security measures.

What to do

The companies with the best cyber posture are typically those that view cybersecurity as an enabler and not simply as a cost of doing business.

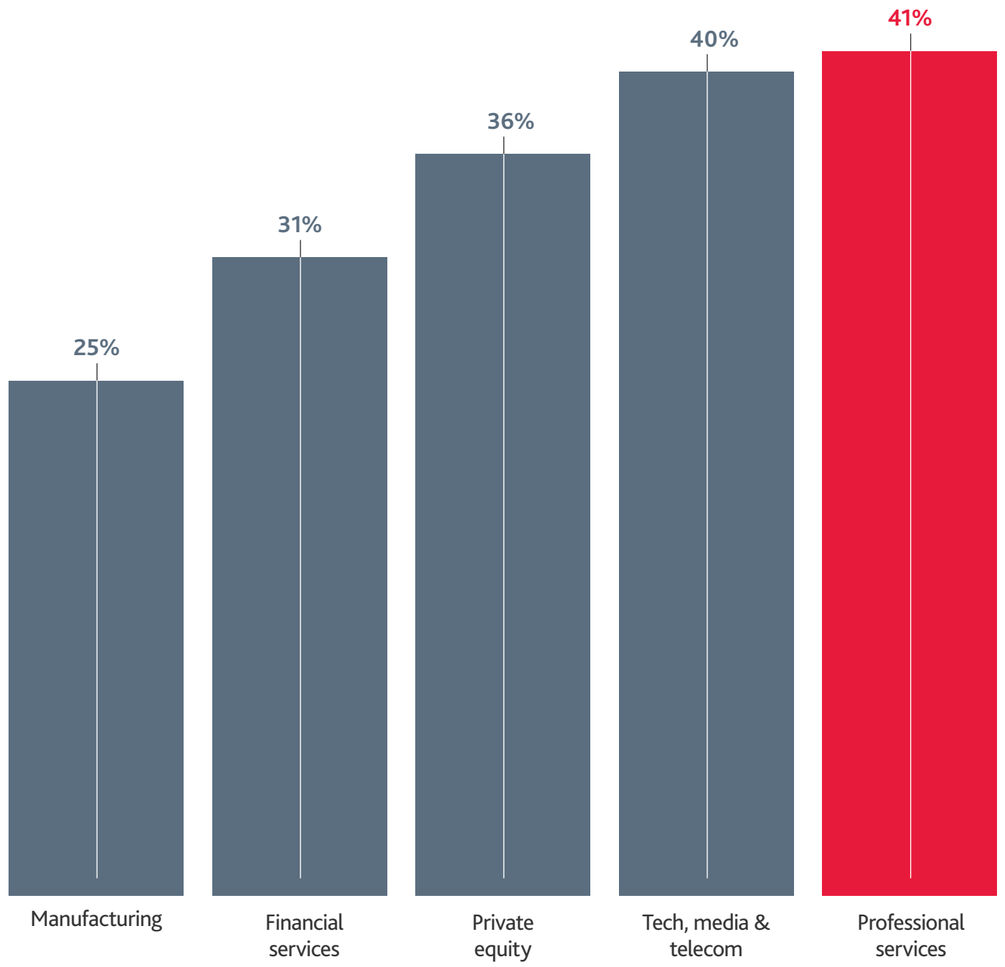
The threat of cyberattacks is making CEOs more nervous than ever. The average cost of a data breach in 2024 was almost $5 million, according to an IBM/ Ponemon Institute report. Against this backdrop, a quarter of CEOs cited cyberattacks as one of their top three risks, up from 19% last year.

"There isn't a lot that is new, it's more the sophistication and the velocity at which some of these cyberattacks are able to penetrate and impact companies that is changing," said Lianne Appelt, Head of Enterprise Risk Management at

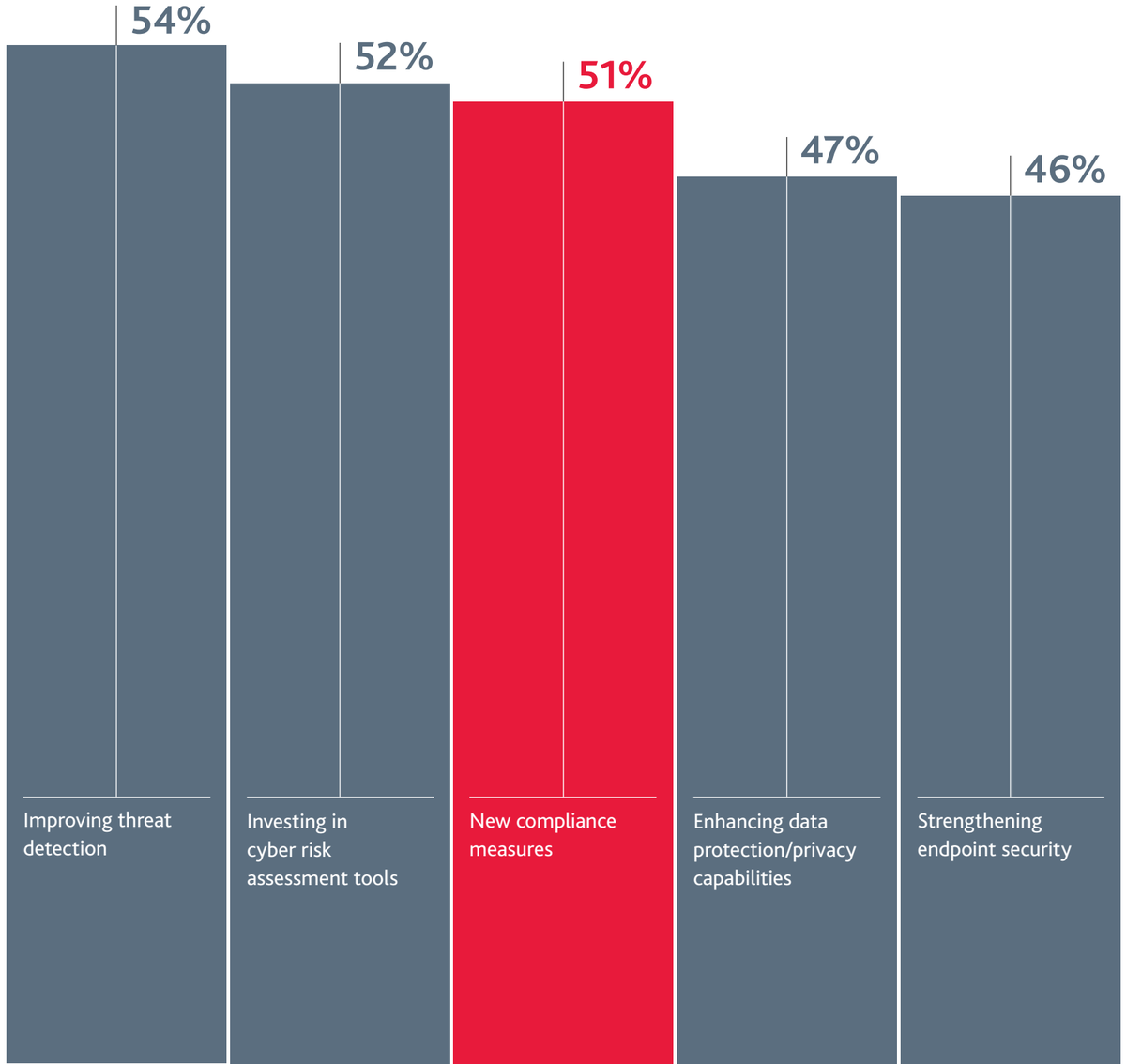
25% of CEOs cite cybercrime as a top three risk against

19% in 2024

THE INDUSTRIES THAT ARE MOST LIKELY TO SAY THEY ARE UNPREPARED FOR CYBER RISK



WHAT ARE BUSINESS LEADERS' CYBERSECURITY PRIORITIES FOR THE NEXT TWO YEARS?



Salesforce. "As a tech company, cyber risk is always at the forefront for us, so we do everything we can to ensure that our products and services and our internal systems are safe."

While email phishing campaigns to launch malware attacks, invoice or payment fraud are still the biggest cyber-related risks, there is an increase in social engineering attacks that target employees. These seek to gather intelligence on businesses to either steal intellectual property or commit some kind of fraud.

"Threat actors are using the machines that we use to make our lives more efficient to help them with reconnaissance and to learn more about the organisation and its people," said Rocco Galletto, Partner and Global Head of Cyber at BDO Canada. "We have a team that tests everything from physical to logical security controls, and they're getting to the point where even malware is now caught by the tools, but social engineering through an employee always gets us in." ▶

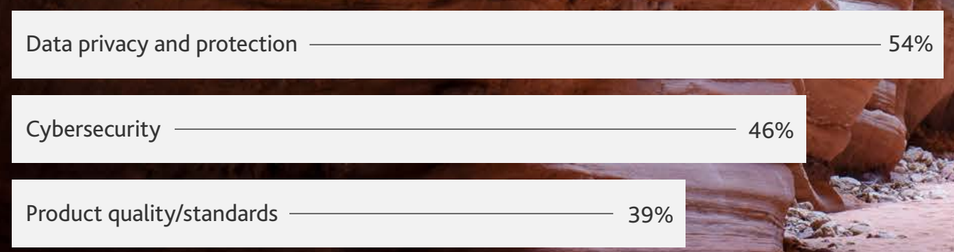
> "When cyber teams are strongly aligned with overarching organisational goals, they can quickly help their organisations stay safe."
>
> **Rocco Galletto,**
> Partner and Global Head of Cyber, BDO Canada

Some industries are potentially more vulnerable than others. Professional services firms were the most likely to be unprepared for cyber risk (41%), followed by tech, media and telecom businesses (40%) and private equity (36%).

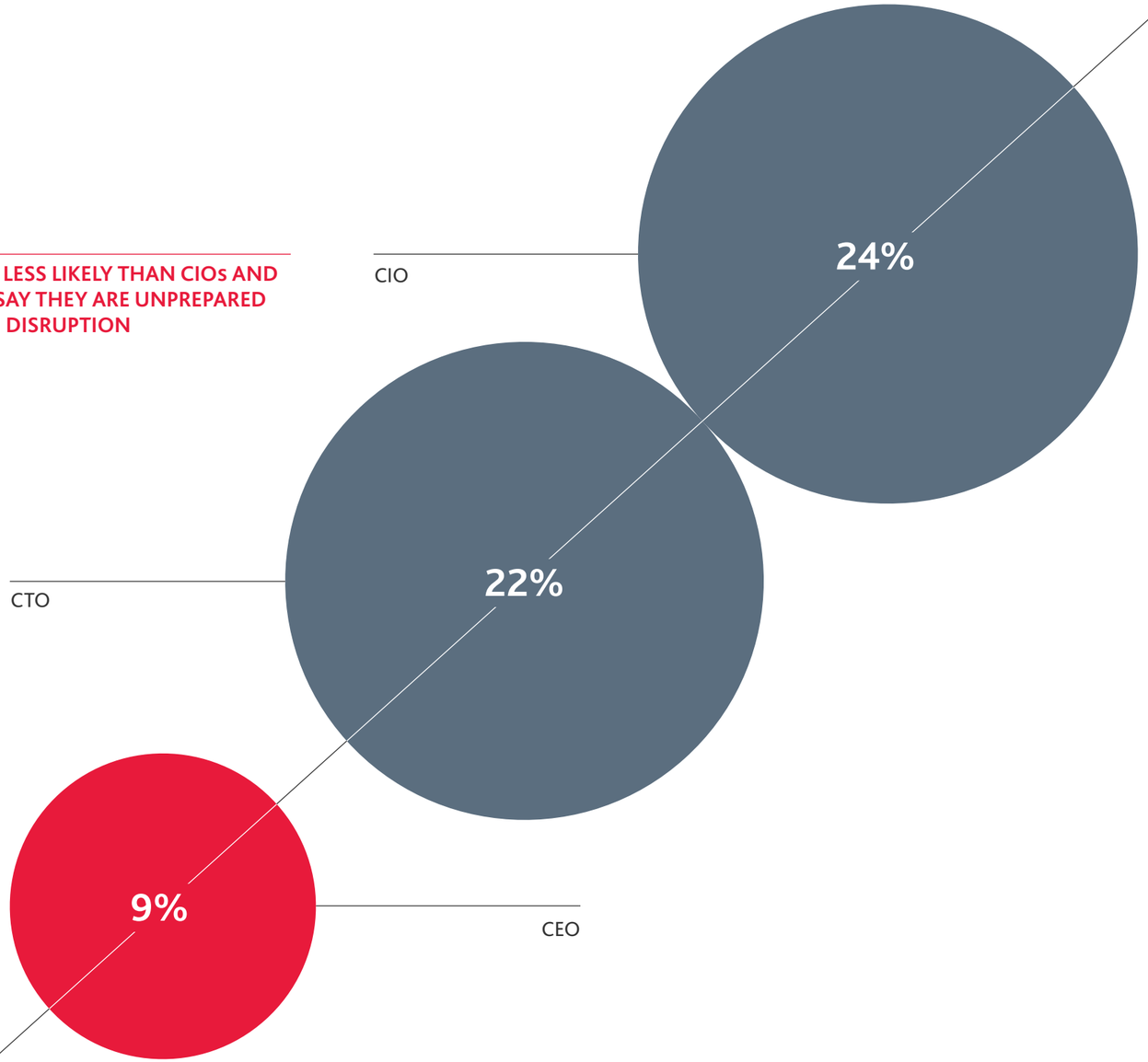
The pace at which cyber threats are evolving means there is also a growing gap between those who are prepared and more cyber resilient and those who are not taking sufficient steps to improve. The pace of tech change is also a risk for companies: 20% of respondents cited this as a top three risk they are unprepared for, but only 9% of CEOs.

"As the tech changes, a business's risk profile changes, not only because the tech is changing, but because of the way they operate changes," said Galletto.

WHICH RISKS ARE EXECUTIVES MOST STRUGGLING TO HANDLE?



CEOs ARE LESS LIKELY THAN CIOs AND CTOs TO SAY THEY ARE UNPREPARED FOR TECH DISRUPTION



"Because tech is moving faster, businesses are moving faster, and cyber has a tough time catching up. So there probably is more of a lag today than there has been in the past – and that gap seems to be getting larger."

The key difference between cyber-resilient businesses and those that are lagging is that the former look at cybersecurity as an enabler to the business, said Galletto.

"When cyber teams are strongly aligned with overarching organisational goals, they can quickly help their organisations stay safe," he said. "This means you can start to anticipate what could go wrong, and if it does go wrong, it can quickly be recovered."

Aside from the real risk of attacks, cyber is also becoming a growing compliance challenge, with 52% of Chief Technology Officers saying their firm has a box-ticking mentality, which can distract from broader risk management strategies.

"Aside from the real risk of attacks, cyber is also becoming a growing compliance challenge."

"Firms go through this check-box exercise, but what they fail to achieve is day-to-day sustainment," said Galletto. "You need people to manage those compliance actions, not just when you're being audited. So it becomes a resource challenge where there just aren't enough people to keep up with sustainment and compliance ends up becoming a check-box exercise." ■

Insight

The cyber challenge for mid-sized firms

Rocco Galletto
Partner, Global Head of Cyber,
BDO Canada

"A frequent challenge for our mid-size enterprise clients is that they are subject to similar regulations as a large enterprise, but they only have small teams – maybe five to ten security people – whose mandate is to keep the organisation safe.

So the organisation may well have 2,000 to 4,000 people, but they only have a small team of security practitioners protecting the business.

Given those circumstances, we're seeing an increasing trend among those types of businesses reaching out to professional services firms like BDO to help shepherd them through some of the areas where they may lack resource capacity or have a lack of understanding of how other organisations of their size are managing or tackling the problem.

Having a structured cybersecurity programme in place is important for organisations to stay ahead or at least keep pace with evolving cyber risk.

There are different levels of readiness that they should consider. The first level is identifying all the things you need to protect within your organisation and how those are protected. It's also important to adapt: when an organisation changes or evolves, security controls must also evolve to maintain its cybersecurity posture." ■

Bridging the risk and reward gap on AI

Companies must get the risk framework right as optimism fuels AI arms race

At a glance

What is changing

Companies are increasingly optimistic about the opportunities created by AI while seeing it less as a risk.

Why it matters

Businesses may overlook or underestimate potential AI risk that could impact them, causing lasting reputational damage and/or severe regulatory entanglements.

What to do

Businesses need a structured risk management framework to safely embrace AI innovation, because if they get it wrong, it can wipe out the investment completely.

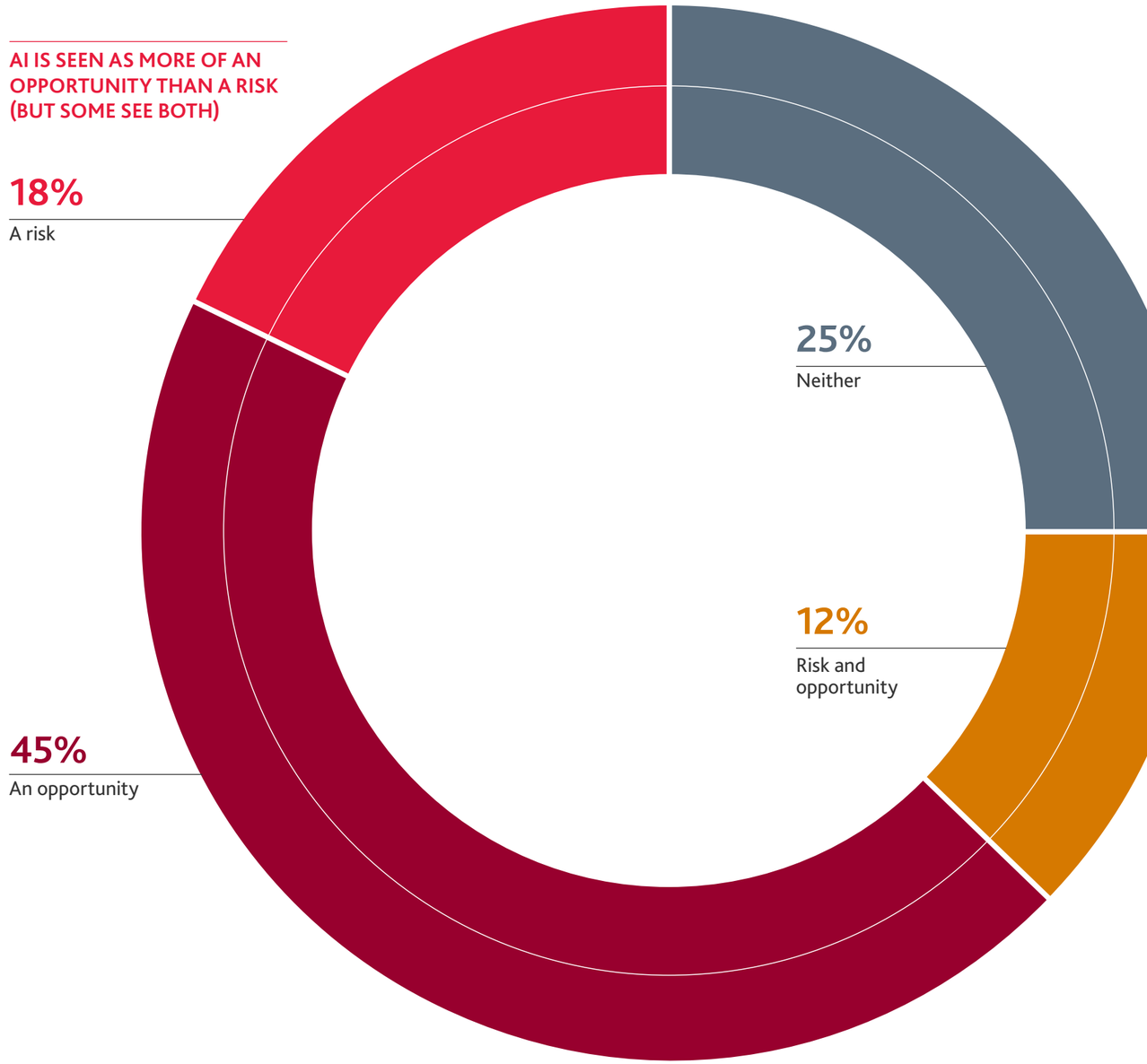
As AI has continued to advance over the past 12 months, attitudes towards the technology's risk have shifted again, with most executives now seeing more opportunity and less risk. Asked to rank AI risk on a scale of one to five, with five as the most significant, most respondents (57%) scored AI risk at three. A year ago, 52% placed AI risk at four.

"We're at a pivotal moment where AI is no longer theoretical - it's in everyone's hands. That accessibility is fuelling innovation, but it's also creating blind spots. As enthusiasm grows, the real risk is assuming AI is plug-and-play. Without a strong risk framework, companies may be scaling exposure faster than they're scaling value," said Kirstie Tiernan, AI Leader at BDO USA.

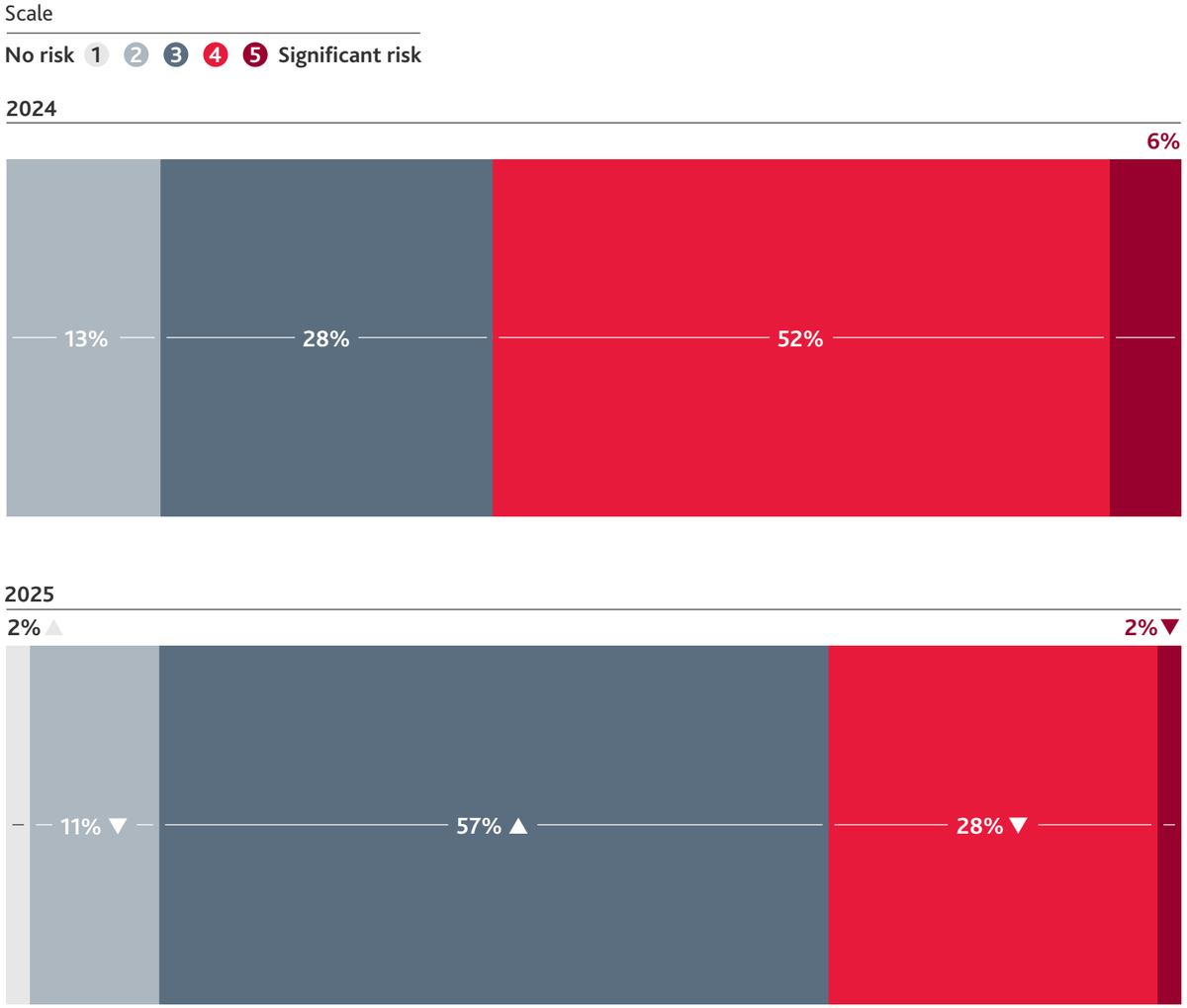
Another reason for this shift is that businesses may believe there is a greater risk of being left behind if they don't embrace potential AI opportunities, added Vernie Balasubramaniam, Director of AI, Privacy and Data Protection at BDO UK.

Part of the issue is that AI is so pervasive across different business needs that senior executives are not aware of ▶

AI IS SEEN AS MORE OF AN OPPORTUNITY THAN A RISK (BUT SOME SEE BOTH)



CONCERNS ABOUT AI RISK HAVE EASED SINCE 2024



everything that is available and therefore fret they may be at a disadvantage to their peers, she said. There are several areas where executives believe AI will have a significant impact on their business over the next 12 months, with cybersecurity coming out on top (55%), followed by compliance monitoring (52%) and supply chain (50%).

"AI-driven compliance is a good thing – you can have more data points to give you much more detailed insight as to a particular risk and who's exposing an organisation," said Balasubramaniam. "This means you can have real-time risk management in areas such as fraud detection."

Despite this opportunity, only 31% of respondents believe AI could help with risk identification or fraud detection and prevention, a potential missed opportunity which again signposts a lack of awareness of the tools that are available.

While there is more optimism among executives, there is still a recognition of the potential risks of using the technology. Some 62% of respondents said AI could increase privacy risks, while 56% said it could increase cybersecurity risks.

It's possible that other risks are being overlooked, said Tiernan.

"There's still a lot of underestimation, particularly around operational and ethical bias risk," she said. "Many leaders equate AI risk with data privacy or just model bias, and they stop there. The reality is that risk now includes reputation risk, workforce disruption, over-automation and maybe even sometimes loss of institutional knowledge."

In the same vein, some companies could be underestimating the broader risk to the company if they get their AI strategies wrong.

"They don't see that you can cripple the company, for example if you put all your data in one place – if you have a breach, you've not lost one database, you've lost all of your data," said Balasubramaniam.

To avoid these potential pitfalls, businesses need to ensure there is wide participation in conversations around AI investments, particularly from a risk perspective.

Polly James, Senior Director for Risk Management at Feld Entertainment, said her business has a cross-functional team that weighs the risks and benefits and agrees on guardrails for any new AI initiatives. ▶

"We are proceeding with caution and testing the waters rather than jumping in with both feet," she said. "We are limiting users and building safeguards around who can use it and ensuring that information is not fed into a public model."

There is also a risk that small and mid-size businesses may become over-reliant on AI tools because it may be cheaper for them to use AI rather than hire more human staff.

"In a large corporation, they'll probably get the balance right because they're likely to have a more structured approach for embracing AI, so SMEs are probably at the highest risk," said Balasubramaniam. ■

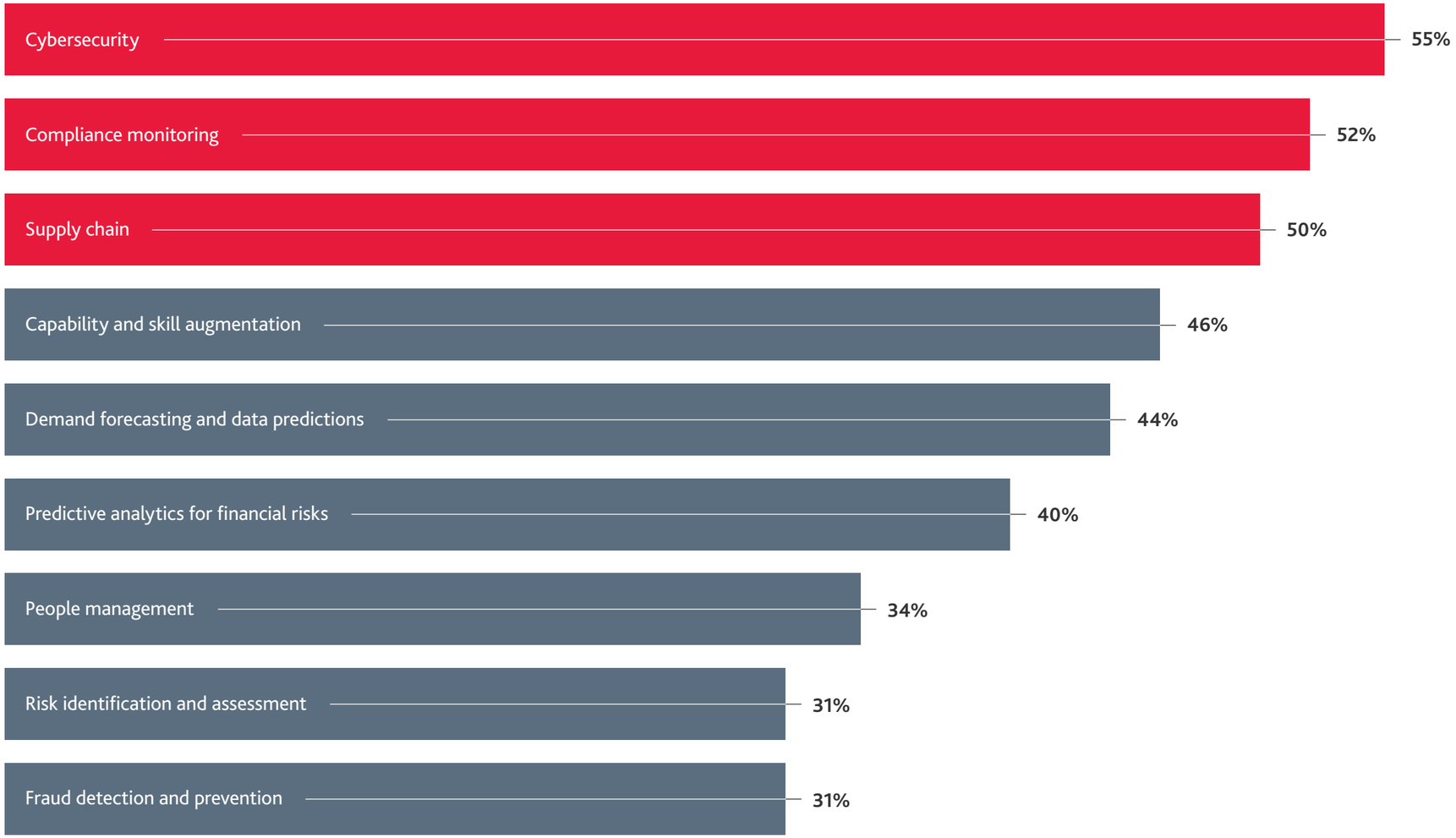
62%

say AI could increase privacy risks

56%

say it could increase cybersecurity risks

WHERE AI IS EXPECTED TO HAVE THE MOST IMPACT IN THE NEXT 12 MONTHS



Insight

A structured approach to AI risk

Vernie Balasubramaniam
Director of AI, Privacy and Data Protection, BDO UK

“We recommend having an AI strategy, someone who is accountable for AI, and an AI governance committee consisting of multiple stakeholders. This ensures it’s not a single point of failure – lots of people are aware and they’re looking at AI from multiple risk opportunities.

It’s also important to implement a structured compliance programme as early as possible to ensure you identify existing controls that can help mitigate any AI risks, so you don’t have to reinvent the wheel. Organisations also need to perform regulation mapping to understand the regulatory impacts globally, not just from a particular location."

Kirstie Tiernan
AI Leader and Member of Board of Directors, BDO USA

"AI risk isn't a technology problem – it's a leadership blind spot. If boards don't know what questions to ask, they can't govern effectively. Organisations need more than a head of AI; they need a governance model that ensures leadership is fluent in the right risk language, and supported by independent oversight on ethics, bias, and accountability. Without that, optimism becomes exposure."

Avoid supply chain ruptures by ‘flexsourcing’

Rising geopolitical risk means organisations need to reassess their supply chains

At a glance

What is changing

Geopolitical tensions and trade war posturing are ramping up concerns about supply chain resilience and making people rethink supplier relationships.

Why it matters

Many businesses were stung during COVID-19 for relying on one supplier far away from their consumers, impacting the availability of their products and their profitability.

What to do

Businesses need to invest in ways to reduce their physical supply chain risk by taking a ‘flexsourcing’ approach that combines nearshoring with friendshoring.

Supply chain risk once again ranked second among the risks business leaders felt unprepared for when the survey was conducted. Since then, global disruptions, including an escalating trade war between the US and countries that were previously seen as trade partners, are likely to have intensified those concerns.

Given the potential business disruption caused by supply chain blockages, nearshoring was already a growing trend post-Covid as businesses moved to limit the distance between suppliers and their end customers. Some businesses are now transitioning to an agile mix of nearshoring and friendshoring, or what may better be understood as ‘flexsourcing’.

“Flexsourcing is increasingly important because with all the new tariffs that are being proposed, you’ve got companies that are looking at drastically altering where they manufacture products, which creates a whole different set of compliance issues for companies to run through,” said Dave Arick, Managing Director for Global Risk Management at Sedgwick. “As we saw during Covid, relying on single points of failure is a recipe for disaster. So having flexibility – not just flexing existing suppliers but potentially finding alternatives – is critical given what is happening in the world today.”

Despite this, executives said the main way they are seeking to reduce physical supply chain risk over the next two years is by enhancing due diligence (60%) and digital monitoring (58%), potentially because recalibrating supply lines again is not easy (nearshoring was bottom of the list with just 41%).

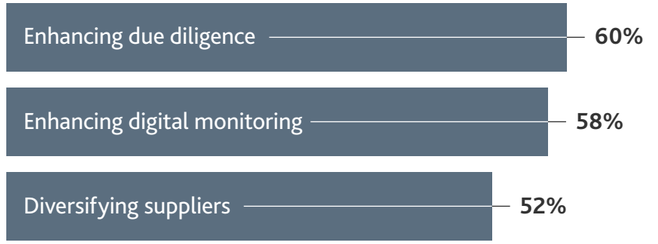
“It’s not a quick win, it’s a long-term strategic play,” said Fraser Paget, Head of Supply Chain and Logistics Advisory at BDO UK. “It also comes down to cost – it’s much better to nearshore, but it’s probably more expensive.”

Executives said they are also strengthening their digital supply chains by conducting regular audits for digital vendors (62%) and investing in enhanced digital monitoring tools and strengthening data-sharing agreements (both 56%).

Whereas in the past there was more investment in digitising finance systems and marketing, logistics is now starting to catch up, said Paget.

“With everything that’s gone on over the past five years, I think that mindset is changing,” he added.

THE TOP THREE WAYS COMPANIES ARE STRENGTHENING THEIR PHYSICAL SUPPLY CHAINS



THE TOP THREE WAYS COMPANIES ARE STRENGTHENING THEIR DIGITAL SUPPLY CHAINS

Insight

Tread carefully on supply chain transformation

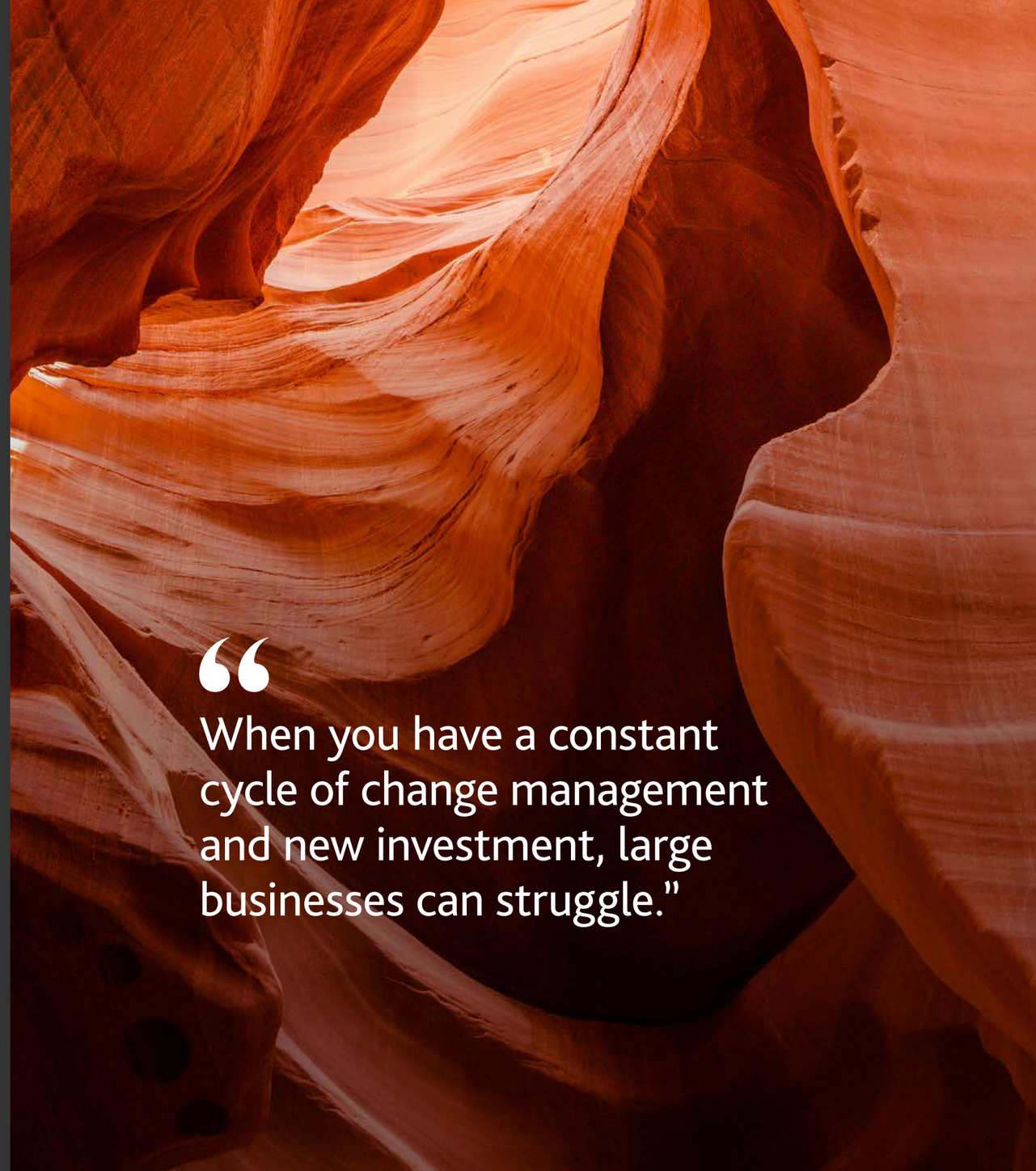
Fraser Paget
Head of Supply Chain and Logistics Advisory, BDO UK

"Supply chain has generally been underinvested from a technology point of view but it's rapidly catching up because it's such a high risk. AI can help massively with forecasting. The challenge is the bigger a business gets, the harder it is to implement new technology or change systems, so you get a lot of large companies running old systems because the change management is just too big – they say we'll just stick with what we've got.

When you have a constant cycle of change management and need for new investment, large businesses can struggle because they can't afford that disruption.

Large-scale transformation projects can significantly disrupt a business's financial performance. For instance, a contributor to Mothercare's demise was the lack of availability of stock after implementing a new warehouse management system, while KFC faced major challenges fulfilling chicken orders when it changed logistics providers. Senior leaders must recognise that investing in technology affects the entire business infrastructure, not just the tech itself.

If you're a grocer and you can't get goods to the supermarket or if you're an e-commerce business and you can't fulfil orders to your customers, then you don't have a business. You have to stress test your technology and risk analyse it and ensure you are able to roll back if things don't go as planned." ■



Fraud risk: don't give fraudsters an opening

The AI boom could increasingly expose organisations to deepfake risk

At a glance

What is changing

The rise of AI is adding to the fraud risk landscape by making it easier for fraudsters to hoodwink staff using deepfake technology.

Why it matters

Employees can be duped into handing over sensitive material or even authorising payments.

What to do

Continuous training on internal controls is essential for reducing fraud risk as most incidents stem from controls not being followed correctly.

Fraud is a potentially underappreciated and sometimes misunderstood risk. Only 15% of executives cited fraud as one of their top three risks, putting it on a par with issues such as brand damage and funding access.

But it can be costly for businesses. Fraud examiners estimate organisations lose 5% of revenue annually to occupational fraud – fraud committed by their own employees – according to the Association of Certified Fraud Examiners (ACFE). On top of that, the rise of AI technology is creating opportunities for professional fraudsters to infiltrate a company using deepfakes. All of this means companies need to pay more attention to fraud risk.

"Sometimes it takes an industry competitor or something in the news or something small that hits home in their own organisation to wake up an organisation." said Glenn Pomerantz, Partner and Global Head of Forensics at BDO USA. "There's no great celebration for the successes of preventing fraud but if you are a victim of a $50 million embezzlement, that becomes very well-known very quickly, so organisations are somewhat inconsistent in respect of their attention to fraud."

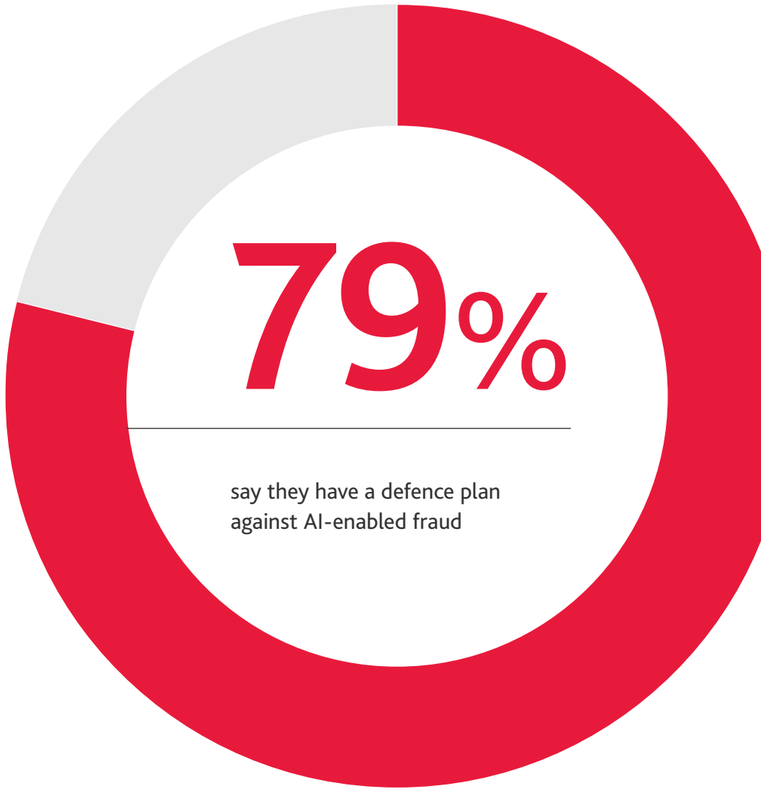
Often fraud occurs not because the right controls were lacking, but because they were not followed properly, Pomerantz said.

"There's always some breakdown – it's almost like death and taxes, it never goes away. But some companies try harder than others," he said.

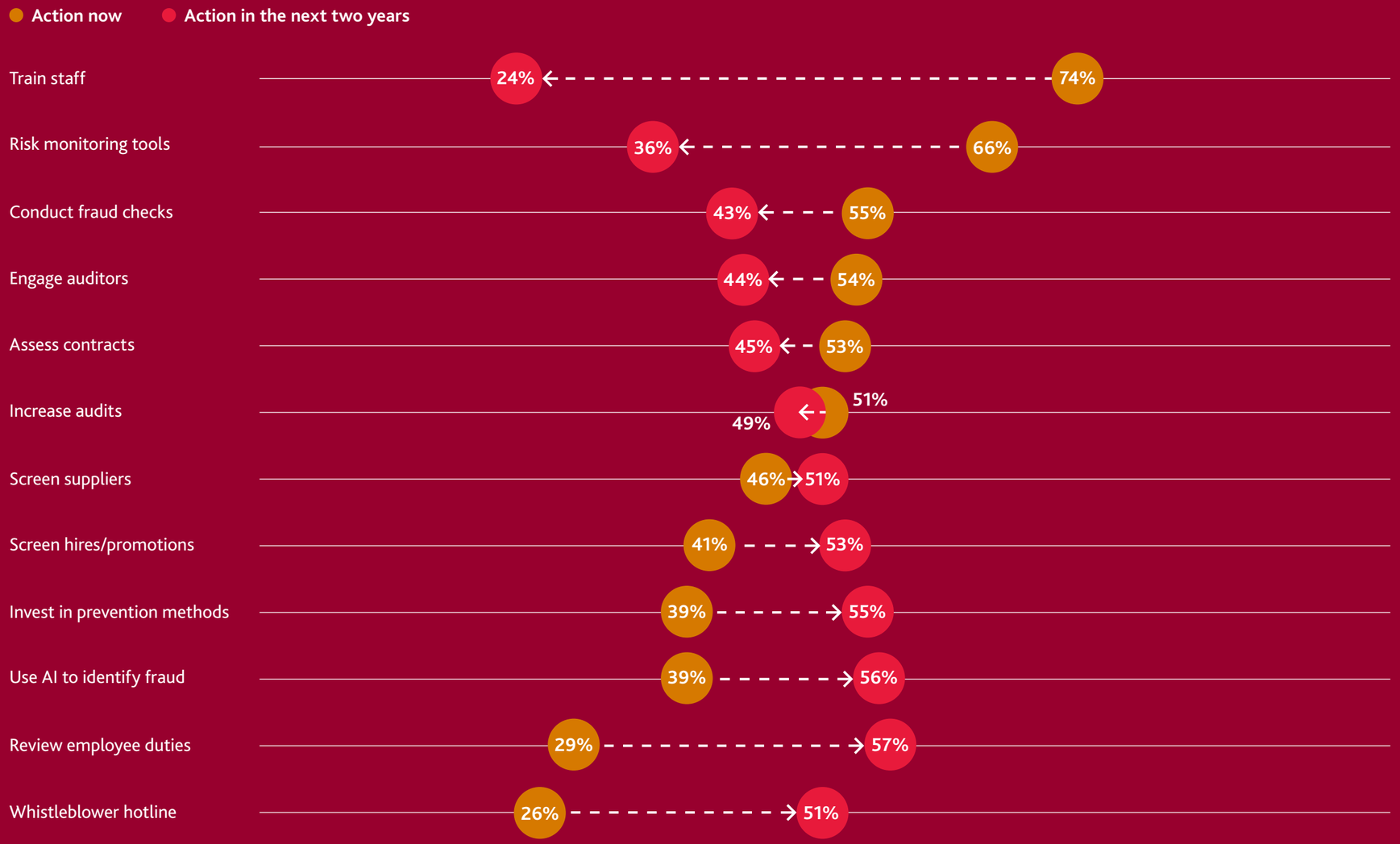
Most companies are taking the threat of AI risk seriously – 79% said they have a plan to combat AI-enabled fraud, though that still leaves a fifth of companies that are potentially vulnerable.

Actions that companies are taking against fraud today include training staff (74%), investing in risk-monitoring tools (66%) and conducting fraud checks (55%). Worryingly, however, when asked what their priorities will be in two years, only 24% said staff training will still be the priority.

"There is potentially a misperception that you only have to train once," said Pomerantz.



ACTION AGAINST FRAUD: TRAINING AND TOOLS ARE TODAY'S PRIORITIES (BUT NOT TOMORROW'S)



dealing with employee turnover – a third of the people you trained three years ago may have moved on. Training has to be reinforced, it's not a one off."

Businesses may also be overlooking an opportunity to detect occupational fraud. Just 26% said installing a whistleblower hotline is a way to combat such fraud, the lowest-ranked tactic in the survey. This is notable because ACFE data shows many frauds (43%) are detected because of tips.

However the anomalous statistic could simply be because many organisations already have functional whistleblower programs, Pomerantz said.

Insight

Busting the myths to reduce fraud risk

Glenn Pomerantz
Partner, Global Head of Forensics,
BDO USA

"Vetting new employees is an internal risk control, whether you're performing background checks and/or checking references.

In several instances insufficient background checks are conducted, combined with a failure to check references. This underscores how critical it is to fully vet potential employees.

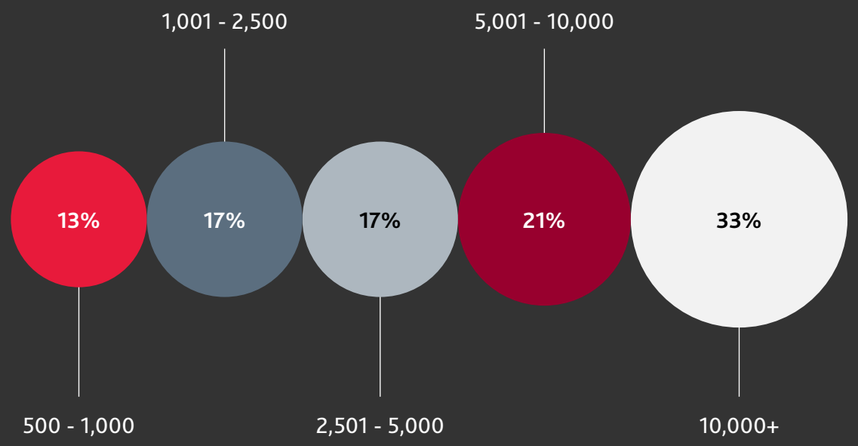
I see organisations along a spectrum, with some checking the background check box in order to fulfil compliance requirements and others conducting intense vetting of employees in positions of trust.

My suggestion is to pick up the phone to the previous employer – maybe 50% will talk to you, and 90% of those 50% will talk to you off the record and provide you with insights that can help you make more informed hiring decisions." ■

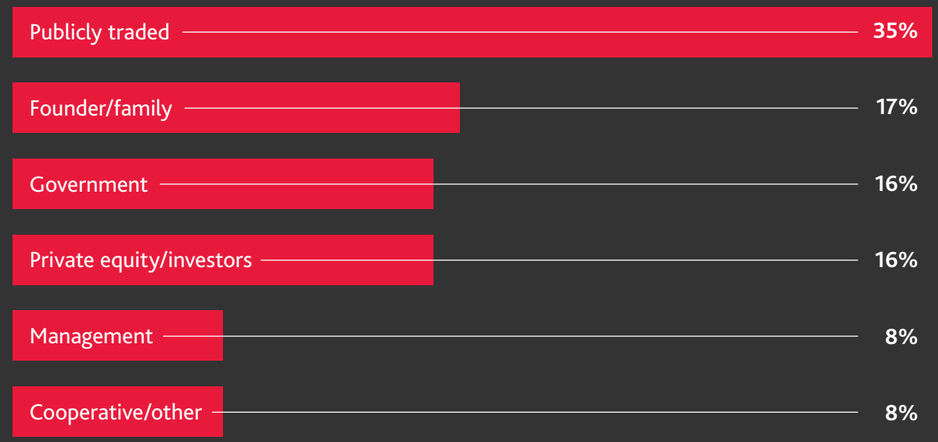
Methodology and demographics

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 by iResearch Consulting Group took place between 24 January and 17 February 2025.

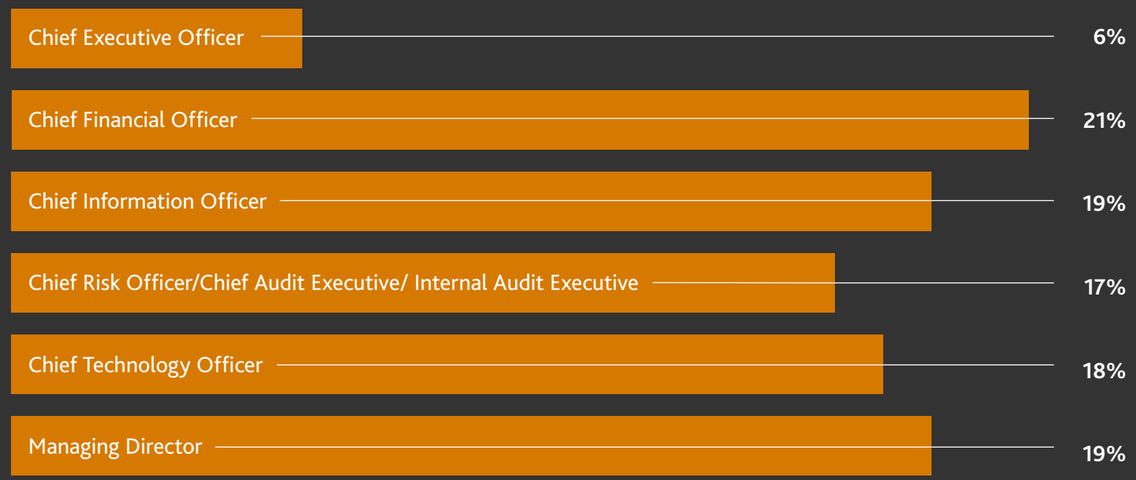
EMPLOYEES



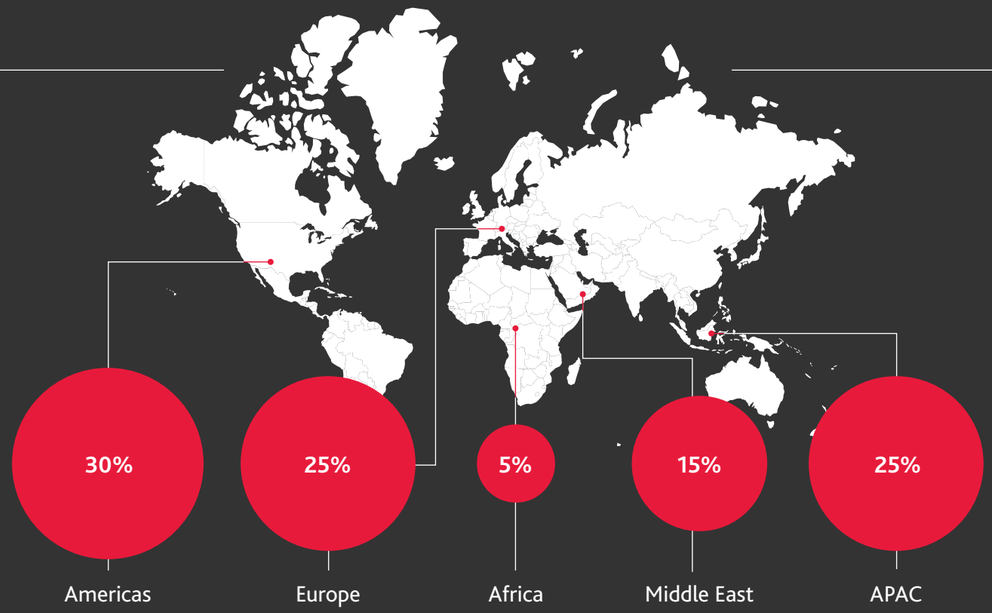
OWNERSHIP



JOB TITLE



LOCATION



FOR MORE INFORMATION:

KOEN CLAESSENS
Global Head of Risk Advisory Services,
BDO Belgium

koen.claessens@bdo.be

www.bdo.global