



GLOBAL RISK LANDSCAPE 2023

THE AGE OF THE RISK MULTIPLIER

FOREWORD

FRESH THINKING ABOUT RISK MANAGEMENT NOT ONLY REDUCES THREATS, IT GIVES ORGANISATIONS THE CONFIDENCE TO PURSUE ADDITIONAL GROWTH



NIGEL BURBIDGE
Partner and the Global Chair
of Risk Advisory Services, BDO
nigel.burbidge@bdo.co.uk



HELGE VUOTI
Partner, Advisory Services, BDO Finland
helge.vuoti@bdo.fi

It's time for businesses to embrace new ways of thinking about risk, looking at the *risk multipliers*, instead of individual risk factors.

That's the key message in this, the 2023 BDO Global Risk Landscape Report. It emerges clearly from the extensive survey of global C-suite executives that provides data for this report and from my BDO colleagues who have contributed here and who, every day, help companies manage risk.

As the data shows, many of the largest companies have already embraced this risk multiplier mindset, which analyses how combinations of risks can be more potent than individual risk factors. But it's time for all companies to think about risks in this more sophisticated way.

This report examines not only the challenges in areas such as AI, digital transformation, human capital, fraud and the threat of climate change, it also aims to equip C-suite readers with information they can use in their organisation to control individual risk factors and multiplier effects.

An improved, more proactive approach to risk is particularly timely as businesses continue to operate in a challenging environment. Russia's invasion of Ukraine has intensified, supply chains remain fragile, cybercriminals are accessing generative AI and other advanced technologies. Also the 2023 World Meteorological Organisation annual report warns that UN climate goals are becoming more difficult to achieve. And all this against a backdrop of weak economic growth, especially in advanced economies, and persistent inflation.

It's important to note that this isn't just defensive thinking. Another message that emerges clearly from this report is that effective risk management, such as putting a risk expert in the C-suite, gives companies the confidence to embrace new possibilities and grow. Yes, it is a time of challenges, many that we cannot or have not anticipated, but it is also an exciting time for businesses to embrace opportunities.

78%

believe the global risk landscape is shaped more by **connections between risks** than individual risk factors

EXECUTIVE SUMMARY

IN AN ERA OF PERPETUAL CRISIS,
BUSINESS LEADERS ARE LEARNING
TO WELCOME RISK

The risk multiplier effect is the way that different risks intersect with and amplify one another. It is not a new concept, but it has come to the forefront in a world increasingly affected by volatility, uncertainty, complexity and ambiguity. This perma-crisis environment means businesses need to consider risks holistically, instead of in isolation, to effectively address them.

In March 2023, the Committee of Sponsoring Organisations of the Treadway Commission (COSO), a US-based private-sector initiative made up of accountancy, auditing and financial executive organisations, released a study with guidance to prevent, detect and manage fraud risk related to external financial reporting. This guidance reflects the move toward a broader strategic risk management approach, linking risk management to business objectives, rather than a narrow prevention-and-compliance approach.

Events, such as the COVID-19 pandemic, Russia's war in Ukraine and geopolitical tensions, highlight the need for a paradigm shift toward a proactive, risk-welcoming approach.



In 12 months, the proportion of executives saying their firm is not prepared for supply chain risk has increased

120%



THERE IS A GRADUAL SHIFT AMONG RISK MANAGEMENT LEADERS TOWARD MORE STRATEGIC, RISK-WELCOMING PRACTICES

Stuart Neil, Director of Strategy and Communications at the International Chamber of Shipping, cites political instability as a major risk multiplier, leading to “increased economic volatility and reducing growth as long-standing policies, trade arrangements and relationships are eroded.” He concludes: “In turbulent times, leaders need to move quickly to navigate and succeed.”

Instead of viewing risks in isolation or trying to prevent every risk from affecting operations, organisations should view risks as opportunities rather than challenges. This evolution in risk management moves from a preventative approach to mitigating inevitable risks in an era of change and upheaval.

The Global Risk Landscape survey showed that while many leaders recognise the concept and importance of risk multipliers, steps to mitigate the impact of inevitable risks are overlooked. Greater openness to risk does not always mean greater preparation. More than half of the executives said their business was particularly unprepared for cyberattacks, computer crime, hacking, viruses, damage to reputation and brand value, economic slowdown and slow recovery or environmental threats.

Increased use of rapidly developing AI has made cyber-risks harder to control, often intersecting with other risks. Opportunities for fraud increase with wider access to AI technology, as well as issues with data quality, reliability and interpretation.

Other risk multipliers to be embraced include workforce and climate risks, which intersect with supply chain, economic, brand value and reputational risks. Novel challenges are emerging, such as protecting global supply chains from Internet of Things (IoT) cyberattacks or mitigating the impact of these often inevitable attacks.

Organisations need to go beyond traditional risk management approaches and recognise the different lenses that can be applied in multiplier risks. However, this new way of working and thinking can be difficult to communicate to stakeholders.

Managing the impact of multiple and intersecting risks requires embracing them, even when they combine or amplify each other and risk velocity increases. Eighty-four percent of respondents agree that risks are becoming more interconnected and complex and 63% say risk velocity is rising. Organisations should be aware of how quickly risks can occur and multiply and be prepared to deal with such threats.

For many organisations, the focus on making sure no disasters happen remains prevalent. However, there is a gradual shift among risk management leaders toward strategic, risk-welcoming practices, rather than just defensive, preventative, and compliance-driven approaches.

Moving toward a risk multiplier approach involves accessing risk, steering away from binary certainties, and favouring likelihoods and probabilities. Maintaining a defensive approach focused on short-term prevention and regulatory compliance is now a less viable risk management strategy. Instead, a dynamic, proactive, forward-thinking approach is needed to address systemic risks in a perma-crisis world.

WHICH RISKS DO EXECUTIVES SAY THEIR COMPANY IS LEAST PREPARED FOR?

The top four risks were given equal ranking

14%



Cyberattacks and computer crime

Damage to reputation or brand

Economic slowdown or a slow recovery

Environmental risk

CONTENTS AND KEY HIGHLIGHTS

P6 | THE RISK MULTIPLIER EFFECT

84%



think risks are becoming more interconnected and complex

P10 | THE ULTIMATE RISK MULTIPLIERS

85%



said their risk management is focused on the connections between risks

P12 | FRAUD FALLOUT

24%



of Chief Executive Officers said cyber-fraud and hacking was their number one fraud vulnerability

P14 | NORFOLK SOUTHERN'S RISK CASCADE

\$400m+

the clean up and legal costs for Norfolk Southern's risk cascade (so far)

P15 | CHAOS AS A LADDER

222%

increase in respondents who said their organisation was 'very proactive' in dealing with risk

P17 | A NEW HORIZON FOR WORKFORCE RISK

Only
19%

offer their employees the chance to participate in social responsibility projects

P19 | CLIMATE RISK SOLIDIFIES



44%
believe climate change poses an existential risk to their business

P21 | GENERATIVE AI: TOMORROW'S RISK MULTIPLIER

86%



of Chief Technology Officers believe AI represents a 'somewhat significant' or 'significant' opportunity for their business

THE RISK MULTIPLIER EFFECT

EMBRACING A NEW PARADIGM FOR GLOBAL RISK MANAGEMENT

The risk multiplier effect represents a paradigm shift for risk management. It describes the way different risks intersect with each other and amplify one another, challenging business leaders to move away from a predominantly preventative approach to focusing on mitigating inevitable risks in an era where change and upheaval are unavoidable and constant. In this environment, new challenges emerge, and risks spread across organisations.

Our Global Risk Landscape 2023 survey showed that while many leaders recognise the concept of risk multipliers and their importance, seventy-eight percent of respondents say the global risk landscape is best characterised by the connections between risks, rather than the risks themselves, with 70% saying their organisation views risks as intertwined. These are key steps in the journey to insulate businesses from the impact of inevitable risks being overlooked.

Although 84% of respondents agree that risks are becoming more interconnected and complex and 63% say risk velocity is increasing, there is a disconnect between recognition and moving toward a risk multiplier-focused, risk-welcoming approach.

78%

believe the global risk landscape is shaped more by **connections between risks** than individual risk factors

Organisations need to look beyond the traditional risk management approach and recognise there are different lenses you can apply to embrace the multiplier impact of risks.

However, it can be difficult to communicate this new mindset. Organisations need to embrace multiplier risks and be prepared to mitigate these threats, even though it can become complicated when risks combine and risk velocity changes.

Dr. Zsolt Szelecki, People Advisory Services Leader, BDO UK, says that traditionally risk managers are focused on making sure no disasters happen, which he describes as a “defensive” approach. However, he is seeing “emergent change” among risk management leaders toward “more advanced practices that look beyond defensive or traditional, compliance-driven risk management.”

The paradigm shift toward the risk multiplier approach involves assessing risk and working with probabilities rather than certainties. This concept is something that risk managers, accustomed to a more black-and-white approach, might not be used to embracing.

There are myriad examples to demonstrate the mechanisms by which the risk multiplier effect operates. Here are some of the key ways risks can intersect to impact a business or industry.

CASCADING RISKS

When one risk can trigger a second risk, which can then trigger a third risk and so on, these are cascading risks: a domino effect that can have a serious impact enterprise-wide. Cascading risks can spread rapidly throughout an organisation, often triggering challenges across the length and breadth of the business long before the initial risk factor can be brought under control. This makes them a particularly overwhelming challenge for risk professionals, requiring proactive planning combined with a fast and coordinated response if the domino effect is to be halted.

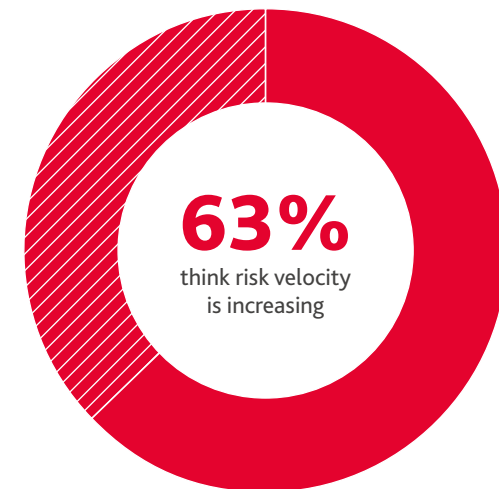
For example, climate risks can trigger technological risks — and amplify further risks — for businesses in a range of ways. Extreme weather events, such as floods, drought and hurricanes, can damage infrastructure, which affects operations, exacerbates supply chain risks, and increases costs. In addition, climate risks are amplifying cyber-risk; many companies have turned to technology to reduce emissions by using AI to optimise operations, but this has increased their online vulnerability. This, in turn, increases the risk of cyberattacks, leading to data breaches, reputational damage and financial loss. These cascading climate and technology-related risks often play out against a backdrop of regulatory risk. As environmental regulations become more stringent worldwide, the cost of compliance can add further costs as businesses are required to reduce emissions, become more energy-efficient and invest in climate-resilient infrastructure.

The COVID-19 pandemic is another example. We saw the knock-on effect of businesses suffering economic loss and workforce cuts when lockdown reduced demand for many goods and services, particularly in the retail and hospitality sectors. For manufacturers, the cascading risk of the pandemic was compounded by supply chain issues, particularly if raw materials were sourced from other countries, along with falling customer demand.



WE ARE BEGINNING TO SEE MORE ADVANCED PRACTICES THAT LOOK BEYOND DEFENSIVE OR TRADITIONAL, COMPLIANCE-DRIVEN RISK MANAGEMENT

DR. ZSOLT SZELECKI
People Advisory Services Leader, BDO UK



RISKS AMPLIFIED

When one risk amplifies the potency of another risk, the ballooning effect presents tough challenges. This often occurs when a new regulation or technology intersects with an existing business risk, amplifying its impact and exacerbating the challenge it poses to an organisation, beyond the levels they may have expected or prepared for. For example, disruptive technology can amplify fraud risks, as criminals use the technology that was designed to help businesses, to develop new ways to phish employees and access internal systems. Your business may not have been prepared for the impact of disruptive technology on business fraud, and your training and protections may prove insufficient to tackle this amplified fraud risk.

Another example is regulatory change, such as increased requirements for Environmental, Social, and Governance (ESG) reporting exposing environmental damage or social governance issues, which then creates amplified reputational risks. One of the best-known examples happened in 2015 when it was revealed that Volkswagen had inaccurately reported its diesel car emissions. This led to a 30% drop in share price, a long process of reputational

recovery and compensation payouts, estimated to be in the tens of billions of dollars, which are still being calculated.

Neil says that a “growing awareness of environmental commitments and reputation management means investor requirements have moved ahead of public leadership.”

No healthy risk management function can do without a serious consideration of ESG. It may not be something that hurts you tomorrow, but it will be in the mid-to-long term.

NOVEL RISKS

The risk multiplier effect can create novel risks that businesses have not dealt with before. One example is the intersection of cyber-risk and supply chain risk with the introduction of Internet of Things (IOT) technology to supply chains. Suddenly businesses had to be cognizant of cyberattacks against their supply chains, opening up a new threat vector that had previously not been on their risk radar.

When SolarWinds, a US-based IT management software company, experienced a supply chain cyberattack in 2020, networks were offline for weeks while malware was removed. Sensitive data was lost, including customer records and financial information.


The company managed to mitigate the damage by promptly disclosing the breach to customers, working closely with investigators, investing in improved security measures and helping customers remove malicious code from their networks. This demonstrates that the appropriate crisis and mitigation response can limit the impact of novel risks.

EXISTENTIAL RISKS


All of these examples of risk multipliers in action, whether it be a cascading chain reaction of risk that starts out small or manageable, amplified risks or novel risks, can snowball into an existential threat that the business may be unprepared to handle, especially when these risks combine and intersect. Our survey respondents ranked business interruption and capital and funding (23.2%), environmental and supply chain (16.6%) and cyberattacks and fraud (13%) as the top three combinations of risk multipliers currently posing the biggest threat to their organisations.

Across real estate and construction, manufacturing, power and utilities, retail and wholesale, oil and gas, and shipping transport and logistics, supply chain risks were cited among their most threatening risk multiplier combinations. Environmental risk also ranks highly, cited by leaders in real estate and construction, manufacturing, oil and gas, and healthcare and life sciences.

It is vital for businesses to recognise that a risk that begins as small and manageable can snowball into an existential risk as a result of the risk multiplier effect. Mitigation strategies, such as detailed scenario planning involving a wide array of teams and internal expertise, and early warning systems that quickly detect risks spilling into other areas of the business, can help predict which risks could pose an existential threat and protect against their spread before it's too late.



84% think risks are becoming more interconnected and complex



70% say their organisation views risks as intertwined

WHAT HAVE COMPANIES DONE TO UNDERSTAND AND MANAGE RISK MULTIPLIERS?

A NEW APPROACH TO RISK

Despite high levels of awareness, especially in regard to supply chain and environmental risks, surprisingly 74% of surveyed business leaders said their organisation does not gather business-wide expertise to understand how risks intersect and multiply. This is a key challenge for industry sectors in the months and years ahead.

Operating against a global backdrop of perma-crisis will require action and a mass-mindset change toward a risk multiplier-driven and risk-welcoming approach, breaking down internal silos and leveraging internal expertise to best protect the business.

When companies discard risk-averse business models, they are often very unprepared and find organisational change overwhelming. The need for change and the steps required need to be interpreted in a way that is understandable to businesses.

Businesses experience and navigate risks daily, but this is not always set out as part of individuals' daily jobs. When this is clearly spelled out and risk management becomes a common language, organisations are more likely to succeed in mitigating multiplier risks.

32%

Conduct audits to identify all potential risk multipliers

55%

Conduct risk assessments that include the multiplier effect

54%

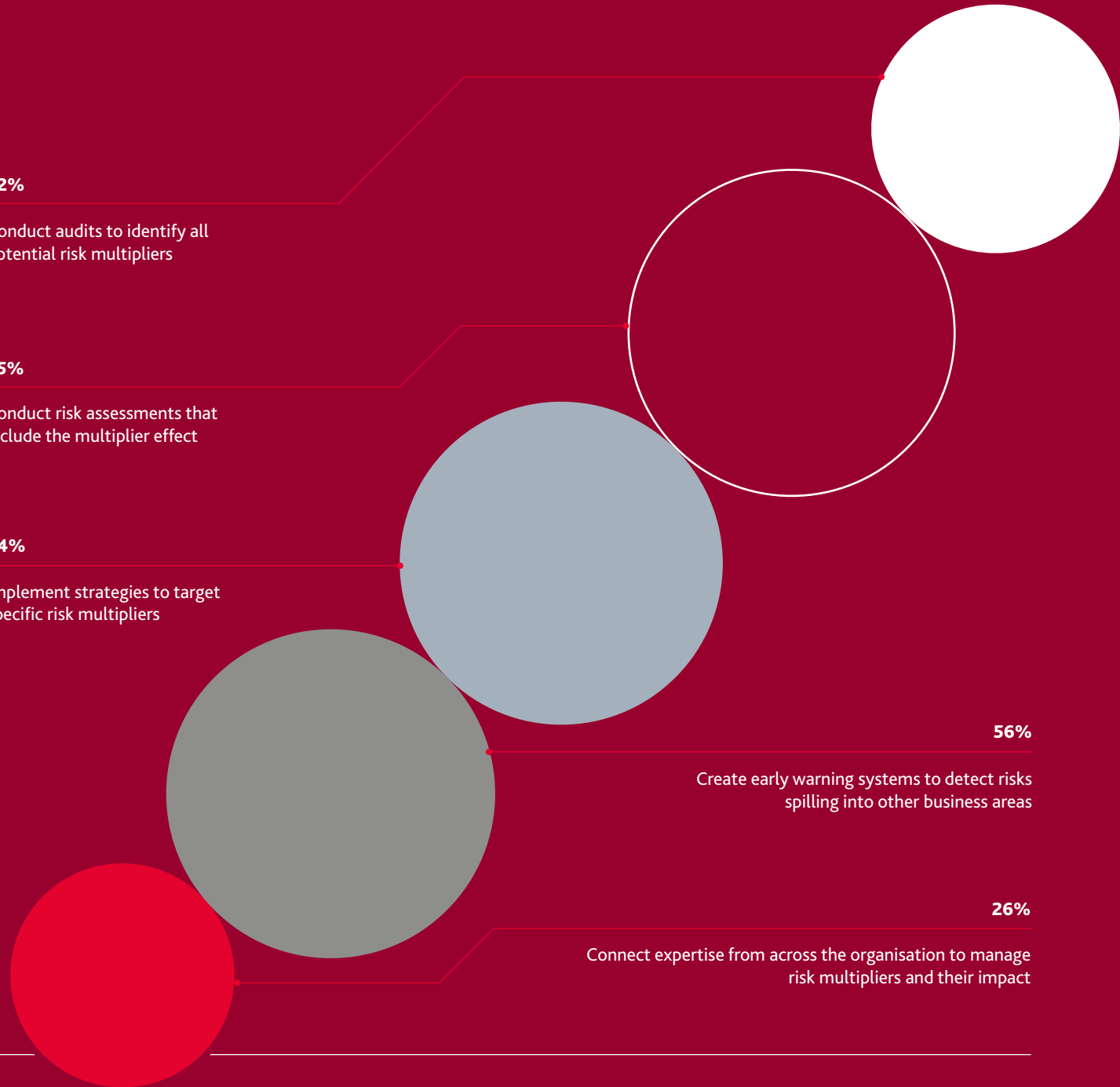
Implement strategies to target specific risk multipliers

56%

Create early warning systems to detect risks spilling into other business areas

26%

Connect expertise from across the organisation to manage risk multipliers and their impact



THE ULTIMATE RISK MULTIPLIERS

THE STICKEST RISKS AND THE THREATS TO YOUR BUSINESS

WHICH RISK COMBINATIONS POSE THE BIGGEST THREAT?

Business interruption x capital/funding

23%

Environmental x supply chain

17%

Cyberattacks x fraud

13%

Cyberattacks x brand damage

12%

Geopolitics x supply chain

9%

Ultimate risk multipliers are the connected risk pairings, or even triple or quadruple threats, that intersect and amplify each other. Even in a risk-welcoming environment, risks need to be mitigated before they become existential threats.

Business interruption x capital/funding was the most-selected pair of risks. This is no surprise, with business operations at risk from the various global crises and concerns about the banking system. A collapse in lending and investment combined with a pause in business operations would make almost any company collapse.

Certain risks were repeatedly cited by survey respondents among the top risk pairings, such as cyberattacks and supply chain issues.

Widespread concern about cyberattacks reflects increasingly digitised operations worldwide. While digital transformation improves processes and is often cost effective, the risk of cyberattacks requires vigilance and investment to detect criminal activity.

WHICH RISKS CREATE THE MOST POTENT MULTIPLIER EFFECT TODAY?

13%

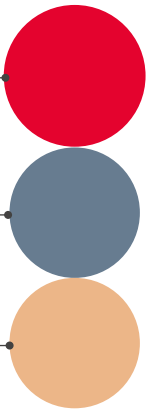
Business interruption

11%

Economic slowdown/slow recovery

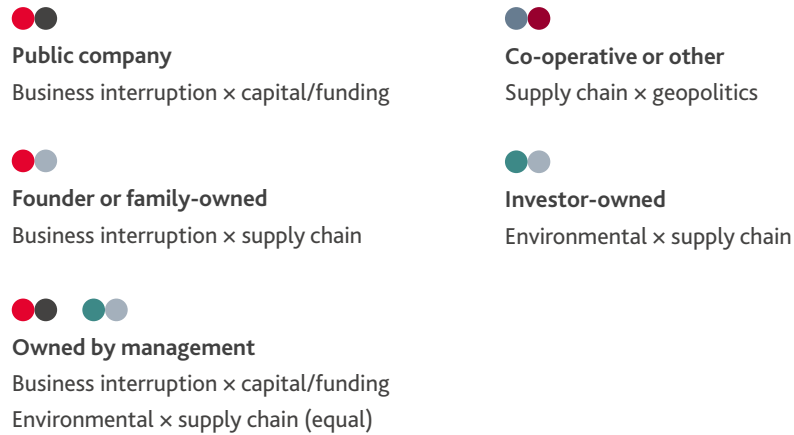
11%

Cyberattacks

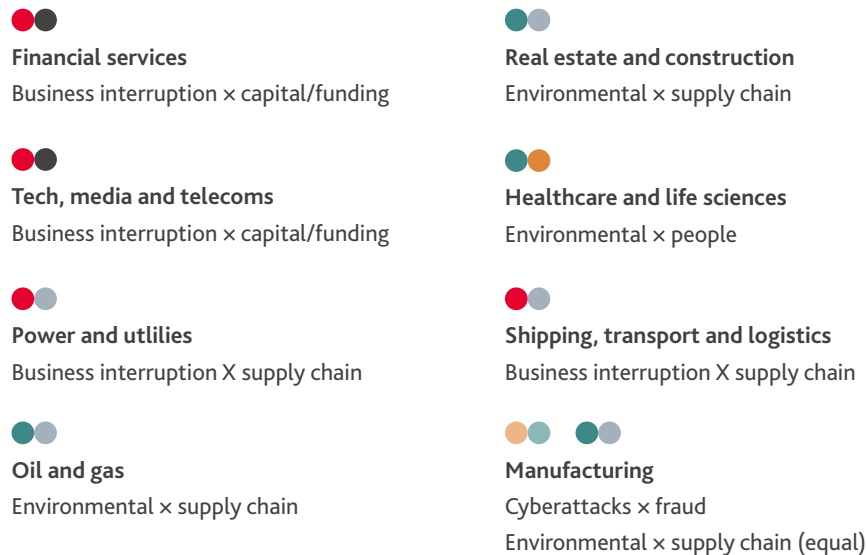


- Business interruption
- Capital/funding
- Cyberattacks
- Environmental
- Fraud
- Geopolitics
- People
- Supply chain

MOST POWERFUL RISK COMBINATION BY TYPE OF COMPANY



MOST POWERFUL RISK COMBINATION BY INDUSTRY



As an ultimate risk multiplier, cyberattack risks intersect with a multitude of other risks. There is the possibility of financial loss, particularly if payment systems are compromised or bank accounts hacked, as well as reputational risk, especially when confidential data is compromised.

Supply chain risks came into sharp focus during the pandemic when the global movement of goods and materials, especially those from China, where some of the world's strictest lockdowns were imposed, was limited. While economies have reopened, supply chain risks continue. As companies rely on sprawling global supply chains, small problems in one location can multiply, triggering larger knock-on effects across borders. Climate risks, for example, can affect supply chains, when the movement of goods and materials is delayed by major weather events, such as hurricanes and other natural disasters.

Russia's invasion of Ukraine, as well as moving away from heavy reliance on supply chains from China, forced many companies to find alternative suppliers. For UK businesses, removing free movement of goods after the vote to leave the EU continues to affect supply chains across industries.

Businesses need to be aware of the most common risk multipliers and dangerous risk pairs affecting their industries, in order to develop the right strategies to protect themselves from financial, environmental, reputational and workforce impacts.

WHICH RISKS WILL CREATE THE MOST POTENT MULTIPLIER EFFECT IN THREE YEARS?

14% | Business interruption

13% | Capital funding

13% | Cyberattacks

FRAUD FALLOUT

HOW TO PREVENT FRAUD IN AN ERA OF INNOVATIVE TECHNOLOGIES AND INTERSECTING RISKS

Fraud is evolving dramatically due to the pace of technological change. This creates intersectional risks with innovations, such as generative AI, aiding both businesses and criminals. Fraud and reputational risk need to be considered as a constant risk pairing for businesses as one regularly triggers the other.

Legacy fraud, such as inventory theft and shrinkage, and intellectual property theft, remain risks, but AI has paved the way for new risks associated with digital transformation and remote workers committing crimes that can be harder to detect. Increasingly cunning, rapid and far-reaching technology-driven fraud threatens businesses, especially when combined with other risks, such as cyberattacks, geopolitical challenges, regulatory risk and reputational dangers.

The Global Risk Landscape survey found that 46% of businesses feel their biggest fraud threat comes from cyber-fraud and hacking. The next two major fraud risks are legacy crimes — inventory theft and shrinkage, and intellectual property theft both at 37% — followed by sanctions fraud at 33%.

When asked about risk combinations, 13% of survey respondents cited the pairing of fraud and cyberattacks as their main threat. Digital asset and crypto-fraud were named in the top four fraud risks. Manufacturing sector respondents named fraud as a particular risk in conjunction with cyberattacks, supply chain risks and environmental threats.

GENERATIVE ARTIFICIAL INTELLIGENCE & CYBER-FRAUD

Glenn Pomerantz, Forensic Partner and Global Forensic Leader, BDO USA, says that “new technologies have given rise to new forms of fraud, with varying degrees of impact. Crypto-related fraud, for example, may be something survey respondents recognise from the media, but they may not be affected by it”, he says. However, the rise of AI technologies is something more organisations need to be aware of, despite its benefits.

“AI works both ways. It can work against you because the criminals have it too,” he says.

WHICH TYPES OF FRAUD DO EXECUTIVES FEEL MOST VULNERABLE TO?

Executives could pick three options

1. Cyber-fraud and hacking
2. Inventory theft and shrinkage
2. Intellectual property theft
3. Sanctions fraud

46%

37%

37%

33%

Fraudsters can use AI to steal and manipulate data, leading to crimes, such as identity theft, credit card fraud and intellectual property theft. Fraudulent transactions can be generated via AI, including fake payments, withdrawals of funds and creation of false invoices. Cyberattacks can be launched using AI applications, such as spreading malware or launching mass denial-of-service attacks. Again, these threats intersect with reputational and financial risks, especially when data privacy mechanisms fail.

"It's not really new that anything involving fraud is reputational, but technology compounds how serious fraud is and how important fraud prevention is," says Pomerantz. "Cyber data privacy is a classic example, as is intellectual property. Every fraud risk is a reputational risk as well," he says.

ESG & FINANCIAL REPORTING FRAUD

Pomerantz describes fraud prevention as a "make or break" issue for companies, especially when fraud intersects with cyber security, ESG and financial reporting. Sensitive ESG-related information, especially in large quantities and covering cross-border supply chains, can be vulnerable to fraud, such as data breaches. However, these risks can have a bigger impact on smaller enterprises.

"If someone embezzles a few million dollars and you're a multi-billion dollar company, it's not even going to hit the news," says Pomerantz. But for smaller companies, a newsworthy fraud case can cause reputational damage. He says this can lead smaller companies to not cooperate with prosecutions, instead "sweeping it under the rug and fixing it from happening again, rather than being in the news".

Organisations under pressure to meet ESG goals might be tempted to fraudulently report on progress, so it appears they are hitting targets.

Pomerantz highlights the difference between companies genuinely meeting ESG goals and those wanting to look good: "When you

say, 'Everyone seems to be doing more than us', you start to get the typical pressures that lead to fraud and that leads to greenwashing, and your reputation is worse".

FRAUD PREVENTION

"It is important to have the highest levels of a company, including the audit committee and the board, overseeing fraud prevention," Pomerantz says. "Ultimately, it comes down to early detection, so those detection mechanisms bring it to the right person's attention quickly. Do you have the analytics or AI in place to detect anomalies quickly and get them investigated immediately?"

The survey found that security measures, such as firewalls, encryption and access controls, were the most common step

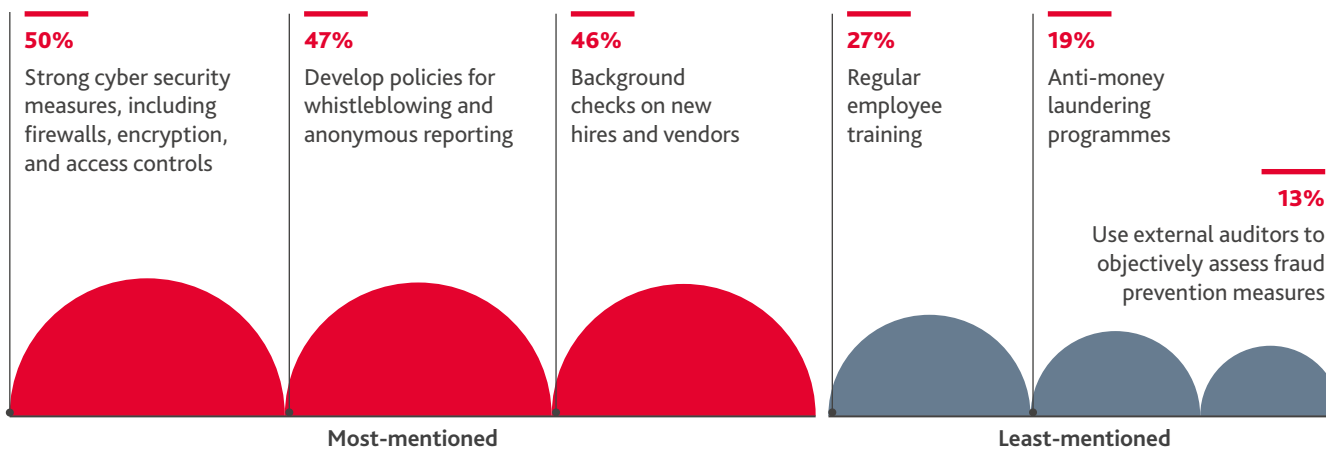
businesses were taking to prevent fraud (50%), followed by developing and enforcing policies for whistleblowing and reporting (47%), and background checks on new hires and vendors (46%).

Pomerantz recommends a culture of "overseeing, plus overseeing on steroids" to prevent and mitigate all fraud risks.

However, the survey found that the least common fraud prevention steps - regular employee training on fraud prevention and detection (27%), anti-money laundering compliance programmes (19%) and external auditing of fraud prevention strategies (13%) - are the ones that would help create this culture of oversight. Businesses that are serious about taking a proactive approach to fraud risks need to take these important steps, especially as criminals become more sophisticated.

WHAT ARE COMPANIES DOING TO PREVENT FRAUD?

Executives could pick three options



NORFOLK SOUTHERN'S RISK CASCADE

A REAL WORLD CASE OF RISK MULTIPLIERS IN ACTION

Global headlines hit the news this February when a Norfolk Southern train carrying hazardous chemicals derailed in the United States at East Palestine, Ohio. Approximately 100,000 gallons of toxic substances, including vinyl chloride, benzene residue and butyl acrylate, spilled across the area and residents within a one-mile radius were hastily evacuated. Officials were forced to undertake a controlled burn-off, polluting the air and surrounding environment.

Norfolk Southern, a US railway operator that generates almost \$10 billion annually, now faces a raft of bad press, lawsuits, new regulations and financial challenges as the spill triggers a cascade of multiplying risks.

The risk multiplier cascade began at the point the train left the tracks with the initial human and environmental damage caused by the derailment and the spill. This, in turn, triggered massive reputational damage with negative press and commentary at a local, regional, national and international level, shaving three points off the business's Dow Jones sentiment driven sustainability score.

Cascading legal and regulatory risks followed swiftly. The company now faces protracted litigation with lawsuits from residents, shareholders and the US government as well as the forthcoming introduction of new stringent regulations such as more frequent safety inspections, minimum crew numbers and mandatory use of failure detection systems.



SOME OF THESE RISKS BEGAN TAKING EFFECT WITHIN MINUTES OF THE SPILL, DEMONSTRATING THE WORRYING VELOCITY AT WHICH RISK MULTIPLIERS CAN TAKE HOLD

The added legal and regulatory compliance costs have compounded the existing financial costs of the spill, with an initial \$6.7bn loss in market capitalisation and hundreds of millions in ongoing clean-up costs. All of these risks were set in motion by the derailment and some began taking effect within minutes of the spill, demonstrating the worrying velocity at which risk multipliers can take hold.

This cocktail of risks brings into sharp focus the consequences of a risk multiplier left unchecked, and a potential failure to recognise and prioritise cascading risks. Bloomberg reported in March that Norfolk Southern's CEO was forced to defend a controversial stock buyback that preceded the incident, insisting that such buybacks don't come at the expense of safety.

Five days earlier, Reuters reported that shareholders filed a lawsuit in an Ohio federal court in which they accused Norfolk Southern of "defrauding them by prioritising profit over safety"

before the disaster, minimising the risks of longer, heavier trains that need fewer workers, and embracing an internal culture that left it open to increased derailments.

Risk multipliers pose existential threats to businesses across all industries. For Norfolk Southern, the reputational and financial damage is expected to continue long term, compounded by reports of further derailments in recent months. While the train was not carrying hazardous substances in these instances, it exacerbated the existing, ongoing and amplifying risks.

The best way to prepare for existential threats is to recognise the threat they pose to your business and embrace the risk multiplier mitigation strategies outlined in this report. Clearly, a more proactive approach to risk management means threats are discovered and their impacts mapped, before damaging incidents occur, so businesses and the environments in which they operate can be protected.

CHAOS AS A LADDER

PUTTING A RISK OFFICER IN THE C-SUITE HELPS TURN THREATS INTO OPPORTUNITIES

Proactive, risk-welcoming management teams are better able to manage and mitigate risk multipliers, and crucially turn risks into opportunities.

Our research discovered that companies with a risk officer in the C-suite are 7.25 times more likely to be risk-welcoming; this factor proved to be more important in driving risk posture than company size or industry sector. For example, companies with more than 10,000 employees are 4.26 times more likely to be risk-welcoming than smaller companies, and this figure drops to 2.2 times more likely for companies in the technology, media and telecommunications sector, compared to other industry sectors.

But industry sector is a driving factor of whether a company employs senior risk officers. In financial services, 82% of respondents say their organisation had a C-suite risk officer (CRO) or similar. This figure is at 71% for the renewables sector. At the other end of the spectrum, professional services and real estate and construction companies are least likely to have a C-suite risk manager at 45% and 48% respectively.

Companies with a risk lead in the C-Suite are 2.1 times more likely to take a proactive approach to risk than those without one. This approach involves proactive planning and embracing the opportunities that can arise from chaos.

Businesses described as “proactive” in dealing with risk are 19% more likely to see risks as intertwined than those described as “reactive”, and three times as many business leaders consider themselves to be risk-welcoming compared to 12 months ago.

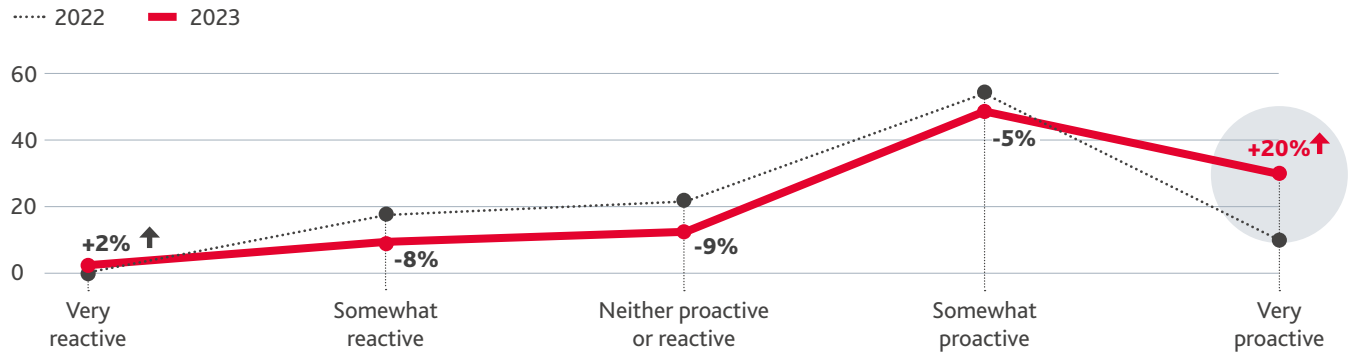
With external risks becoming more severe and unavoidable, forward-thinking risk professionals are pushing their companies to view chaos as a ladder of opportunity, rather than merely a challenge to be surmounted. Tectonic shifts in the risk landscape are opportunities to gain an edge on the competition, adapt faster and become more robust and resilient. In this environment, taking a proactive approach to risk management should be seen as part of an antidote to the risk multiplier effect.

Moving away from a siloed approach helps organisations become more proactive. When businesses operate in silos without involving all key risk owners in risk management, this presents a challenge when talking about inter-dynamic risks, as colleagues never have an opportunity to discuss them together, to understand how they build on each other and see what the potential outcomes can be.



FORWARD-THINKING RISK PROFESSIONALS ARE PUSHING THEIR COMPANIES TO VIEW CHAOS AS A LADDER OF OPPORTUNITY, RATHER THAN MERELY A CHALLENGE TO BE SURMOUNTED

PROACTIVE VS REACTIVE RISK MANAGEMENT



HOW RISK APPETITE IS INCREASING



WHAT FACTORS MAKE A COMPANY RISK-WELCOMING?

If they have a risk officer in the C-suite they are

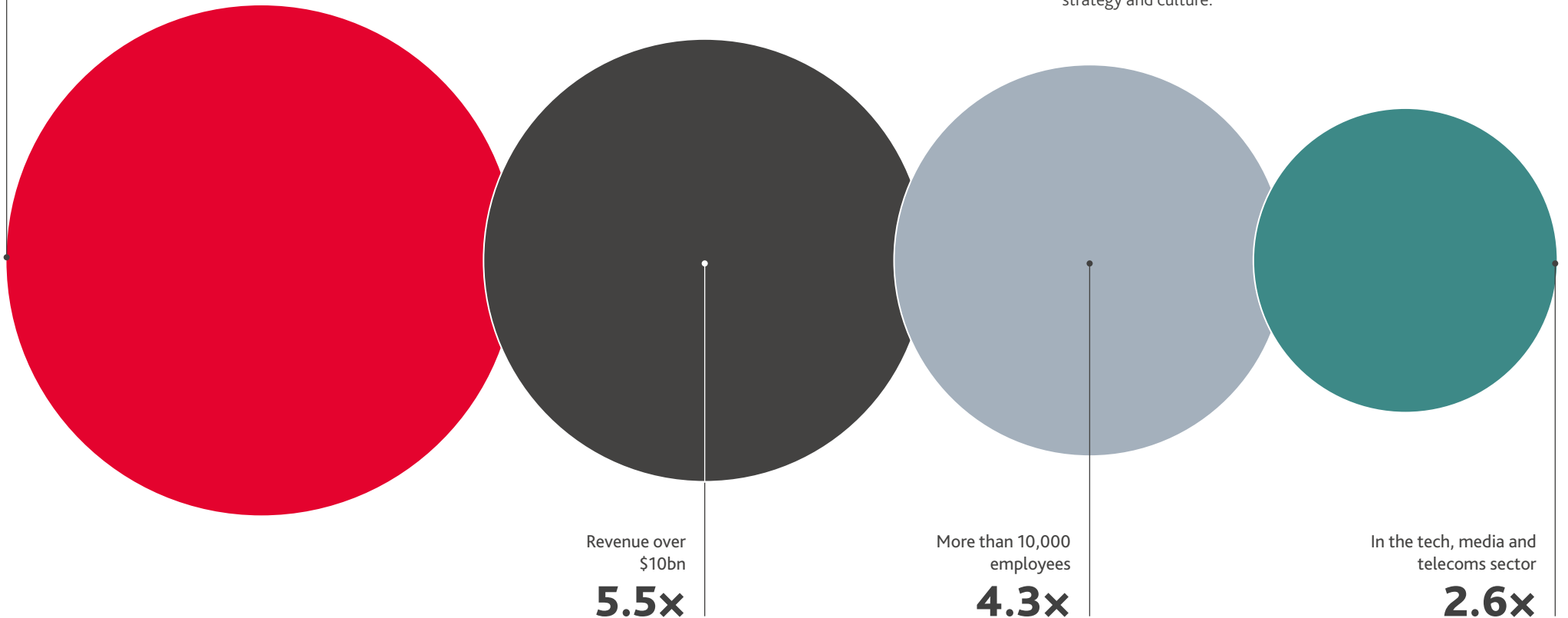
7.3x more likely to welcome risk

Hierarchical, siloed workplaces undermine an organisation's ability to achieve objectives and even stop businesses from operating. But mature organisations link risk management to strategy, so it becomes a priority at all levels, rather than a separate responsibility for a risk management team that operates away from the rest of the business.

Multiplier risks can have fantastic opportunities, but it requires a level of engagement, leaning into risk management. Ultimately, when a business builds risk management as something that helps achieve its objectives, it changes the mindset of how it's viewed and how it can help manage the onset of multiplier risks.

There are many ways companies can turn risks into opportunities. For example, if a business is facing the prospect of losing market share to a competitor, this can be viewed as an opportunity to develop better products and services to appeal to customers. When climate risks increase, such as more frequent floods, investment in mitigation measures and a recovery plan builds resilience for the long term. Investment is also important for mitigating data breach risks. Innovative security measures pay for themselves many times over when they prevent costly and reputationally harmful cyberattacks.

A major part of creating a dynamic, proactive mindset is to ensure risk managers are firmly embedded in the C-suite, while still ensuring risk management becomes part of the entire company's strategy and culture.



A NEW HORIZON FOR WORKFORCE RISK

HUMAN RISK PROFESSIONALS MUST LOOK BEYOND TRADITIONAL SILOS TO MANAGE THREATS

In the age of risk multipliers, HR professionals need to look beyond traditional metrics, such as staff retention and turnover, and take a broader view, focusing on mitigating the impact of intersecting human capital risks, rather than minimising the scope.

However, the Global Risk Landscape survey revealed respondents still consider the top three human capital risks to be largely internally focused, such as health and safety risks (21%), turnover and retention (19%) and employee misconduct (18%). These figures are reflected on a regional basis. Health and safety risks rank in the top two human capital risks for Europe (26%), Middle East (26%), Asia-Pacific (16%) and the Americas (22%). Turnover and retention is in the top two for Europe (22%), Asia-Pacific (25%) and the Americas (22%).

Survey respondents named turnover and retention (47%), contingent worker arrangements (43%) and recruitment challenges (41%) as the main human capital risks in a year's time. For HR professionals to deal with these risks proactively, the intersecting risks that magnify workforce challenges must be examined.

When asked about the biggest risk multipliers by industry, only healthcare and life sciences named people alongside environmental risks. To move toward a risk-welcoming, risk multiplier approach and succeed in this new operating environment, HR professionals must take a more holistic approach and collaborate with people across the business to understand how multiple risks affect hiring and retention. Our research indicates that more needs to be done to develop this approach.

Only 26% of respondents said they bring together expertise from across the organisation to help understand and manage risk multipliers.

HR professionals can manage human capital risks proactively in a risk-welcoming environment. The top priority is agility of mindset, so organisations can adjust quickly to internal and external change.

Connectivity and clear understanding of risks is important. While not all employees are risk management experts, large-scale awareness is vital. This enables company-wide risk management through culture and technology. Culture should be set from the top levels of management, so all employees feel safe to discuss and report concerns. Technology, in turn, can drive effective responses to risks.

“

**NOT EVERYBODY NEEDS TO BE AN EXPERT
ON RISK MANAGEMENT, BUT EVERYBODY
NEEDS TO HAVE THAT AWARENESS.
YOU MAY BE USING DIFFERENT WORDS,
BUT IT ALL CONNECTS**

ALISA VOZNAYA
Head of Risk Transformation, BDO UK



Considering reputational risks means HR professionals need to look at how their organisations remain attractive to potential employees. Reputational risks intersect with other risks that can hinder recruitment, such as the effects on the talent pool of changing demographics and evolving attitudes to issues including climate, human rights and social responsibilities.

For example, intersecting reputational and supply chain risks, such as modern slavery scandals, can influence whether people want to work for a company. The green technology drive can lead to the purchase of solar panels manufactured in poor working conditions. This can, in turn, create corresponding reputational risks, which make employers less appealing to qualified people.

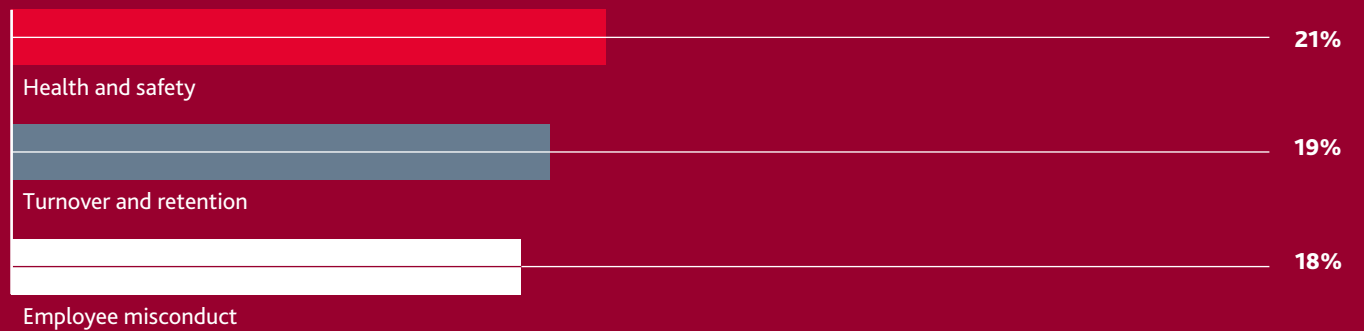
In a market where employees, suppliers and contractors are more discerning about where they choose to work, a company's social capital and reputation for ethical behaviour become real factors in its ability to meet its hiring needs. To mitigate the risk of labour shortages and an inability to employ the best people, risk-welcoming HR professionals, along with management, need to examine all workforce risks through a wider lens.

Additionally, the so-called "great resignation" resulting from the COVID-19 pandemic created a novel risk, in the overheated recruitment market. The perfect storm of not enough trained people and the urgent need to recruit when economies started to reopen, created multiple risks where some demanded higher pay, some accepted more junior roles and some took jobs beyond their experience.

It is vital to recognise the scope of workforce risks that can be affected by external factors and bring in expertise from across the business to identify issues and work together to become a genuine employer of choice for talented workers.

WHAT ARE THE TOP HUMAN CAPITAL RISKS TODAY?

Executives could pick three risks



...and in three years?



CLIMATE RISK SOLIDIFIES

ENVIRONMENTAL THREATS ARE A RISK
MULTIPLIER THAT CANNOT BE IGNORED

Rosemary DiCarlo, the UN Under-Secretary-General for Political and Peace building Affairs referred to climate as the original risk multiplier, in a 2015 address, following the Paris Agreement. Eight years on, her remarks apply to businesses, as well as governments.

“The relationship between climate-related risks and conflict is complex and often intersects with political, social, economic and demographic factors,” she told world leaders. “The risks associated with climate-related disasters do not represent a scenario of some distant future. They are already a reality for millions of people around the globe — and they are not going away.”

Climate risks pose serious and intersecting threats to companies, such as increased costs to meet regulations, mitigate climate change and improve resilience; reputational damage when risks are not taken seriously; costs associated with remedying damage; supply chains disrupted by extreme weather events; and losing customers who move because of climate issues, such as long-term drought.

“

CLIMATE RISK IS HIGHLY IMPORTANT BUT LEADERS
SHOULDN'T LOSE SIGHT OF OTHER ISSUES SUCH AS CHILD
OR FORCED LABOUR IN THE SUPPLY CHAIN, BIODIVERSITY,
AND DATA GOVERNANCE IN THE AI ERA

PIERRE TAILLEFER
National Sustainability and ESG Leader, BDO Canada

Dr. Tara Chittenden, Foresight Manager, The Law Society, outlines how serious climate risks are for organisations globally: "The acute and chronic physical impacts of climate change are a significant risk to business operations, infrastructure, supply chain and beyond."

"Across market verticals, including financial and professional services, manufacturing, utilities, healthcare and more, risk professionals are worried about climate risk," she continues. "The climate crisis is a risk multiplier across society and for the legal sector brings new and wicked problems around attribution, jurisdiction and accountability."

Cascading climate risks trigger further, escalating risks. This has affected a range of industries, such as coastal real estate and tourism businesses affected by hurricanes, agricultural businesses suffering because of prolonged droughts or frequent floods, and insurance companies losing billions as more natural disaster claims are paid. This, in turn, affects businesses financially when their premiums rise.

Among respondents to our survey, three-quarters agree that climate risk poses a significant, short-term risk to their organisation. However, only 69% agree climate change is a significant long-term risk. Given the impact already felt by many industries, it is surprising that these figures are not higher.

Sixty-seven percent of respondents have plans and processes in place to manage the impact of climate change, but 62% of organisations prioritise ESG regulatory compliance over proactively protecting the business from climate risks. Taking a compliance-led

48% say the threat of climate change to business has been exaggerated

approach indicates a disconnect between acknowledging the risk multiplier effects of climate change and effectively managing the risks. Almost half (48%) of respondents say the threat of climate change to businesses has been over-exaggerated.

The climate crisis drives everything that drives regulation, which drives business models. For some energy companies, climate regulation has created an "existential crisis" as executives claim that by 2030 governments say they cannot continue with current infrastructure. With retailers, the climate crisis shifts public opinion, affecting products with limited sustainability, such as single-use plastics and fast fashion.

The intersection with supply chain risks and the need to meet ESG goals is a challenge — 16.6% of survey respondents ranked the pairing of environmental and supply chain risks as the main threat to their organisation.

Climate risk requires scenario-building. This process involves identifying potential risks, assessing likelihood and impact, and developing mitigation plans. Scenarios need to be based on realistic assumptions, using scientific data to estimate the rate of climate change, predicting future regulations, and examining technological developments that may help with forecasting and mitigating the effects of extreme weather events.

As well as scenario-building, businesses need to develop detailed risk management plans that include risk assessments and strategies to reflect the inevitability of climate-related impacts, such as response and contingency plans. It is part of a risk-welcoming approach, along with building resilience in operations and supply chains, and keeping updated on the latest climate science and natural disaster forecasting to be prepared.

In the UK, the [Financial Conduct Authority](#) has taken steps to help companies avoid the risk of greenwashing. Companies will need to ensure accuracy in reporting on sustainability risks, opportunities and

WHAT THE C-SUITE SAYS ON CLIMATE RISK

62% "My organisation prioritises ESG regulatory compliance over proactively protecting the business from climate risk."

67% "My organisation has processes to manage the impact of climate risk."

69% "Climate change poses a significant **long-term** risk to my organisation."

75% "Climate change poses a significant **short-term** risk to my organisation."

impacts, encourage a proactive culture that goes beyond compliance, and minimise reputational risks associated with climate performance. The [Securities and Exchange Commission](#) in the US has launched the Climate and ESG Task Force to develop ways to identify ESG-related misconduct in line with increased investor reliance on transparency in this area.

Businesses need to appreciate the impact of climate risk on their operations and ultimately their long-term growth and survival, so it should be expected that in forthcoming surveys, almost 100% of respondents would recognise the serious short and long-term threats. Your organisation needs to recognise this and enact mitigation strategies, such as scenario-building and forward-thinking technological investment to combat this risk.

GENERATIVE AI: TOMORROW'S RISK MULTIPLIER

THE NEXT GENERATION OF AI CREATES NEW THREATS, BUT BUSINESS LEADERS ARE FUNDAMENTALLY OPTIMISTIC

Since John McCarthy, the American computer scientist, coined the term "artificial intelligence" in 1955, AI technology has evolved and its applications expanded. While embracing generative AI is vital for digital transformation, its risk multiplier potential has grown exponentially.

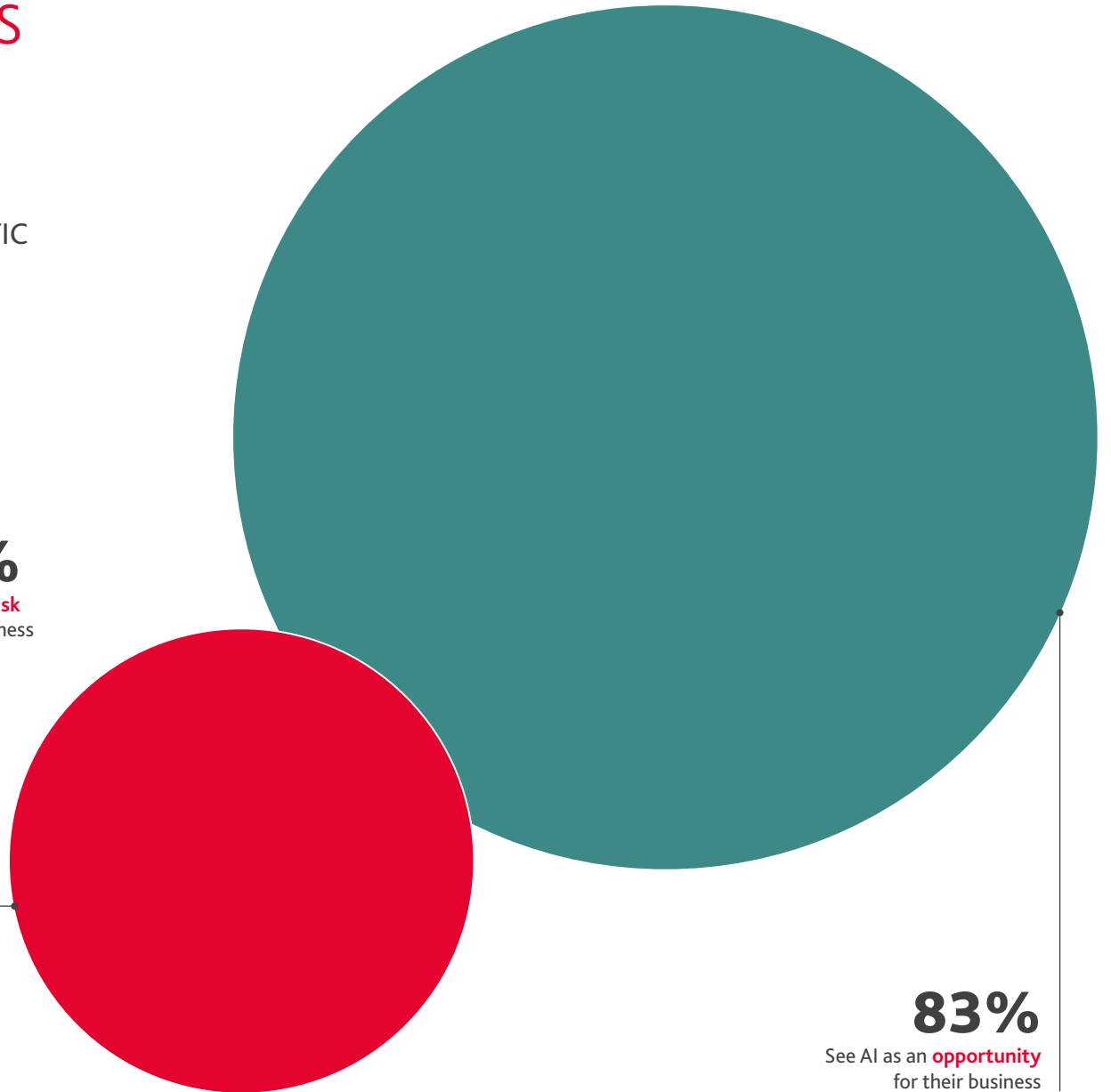
In January, Geoffrey Hinton resigned as leader of Google's AI research division over growing concerns with the technology he helped create. His resignation letter cited concerns about poor accountability and transparency in Google's AI research, and said the company needed to do more to ensure AI is not used for harmful purposes.

The challenge for companies is to balance leveraging AI's enormous benefits with managing the risks, not all of which are fully understood.

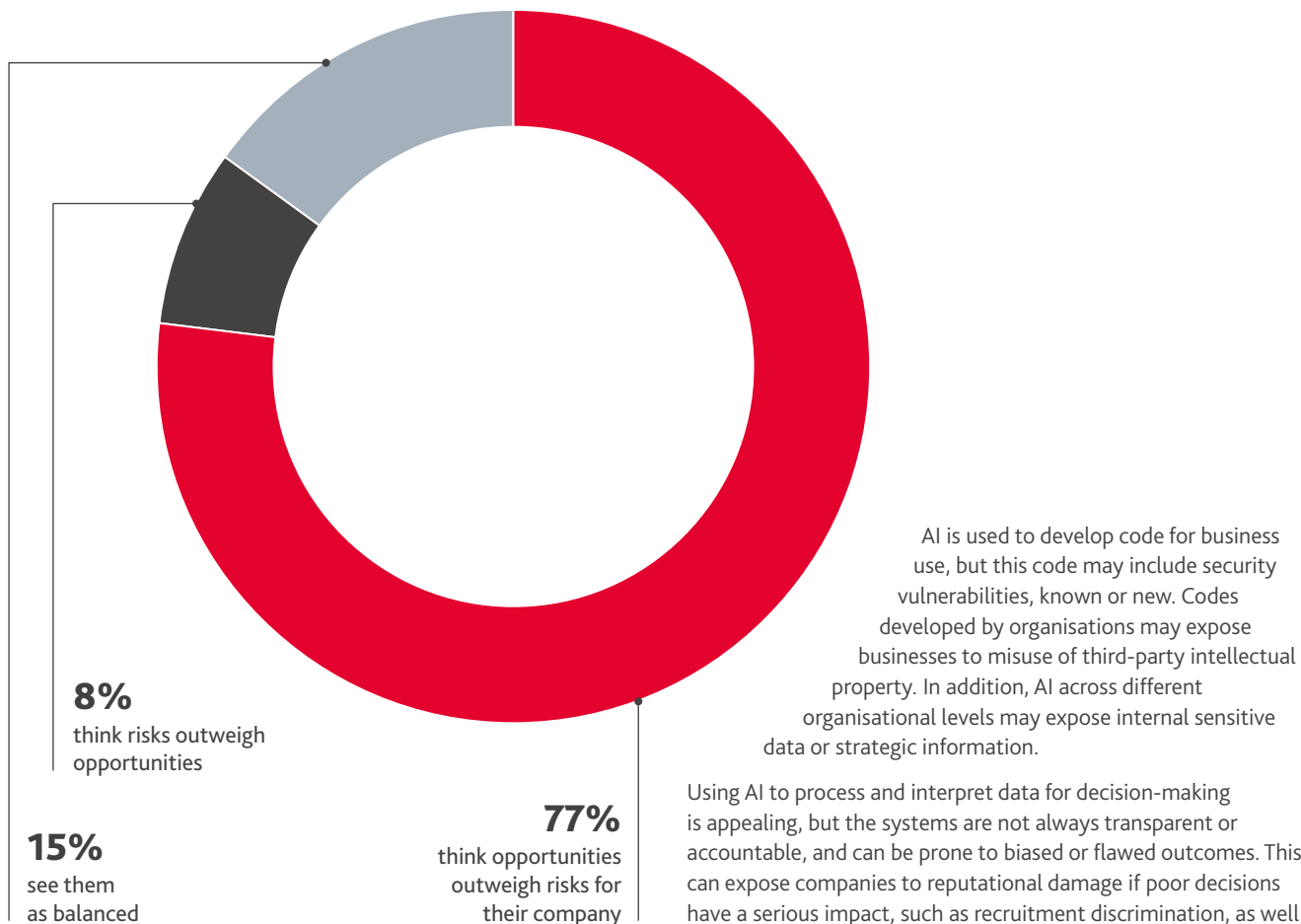
Existing AI-associated cyber-risks include criminals using the technology to develop sophisticated attacks that are difficult to detect and defend. These can be technical, such as manipulating systems and bypassing security measures, or human behavioural, such as manipulating users into making mistakes that expose organisations to cyberattacks.

24%
See AI as a **risk**
to their business

83%
See AI as an **opportunity**
for their business



OPTIMISTS ON AI GREATLY
OUTNUMBER PESSIMISTS



as potential financial, governance and environmental impacts of flawed AI-generated decisions.

A further risk is heavy reliance on AI, leading to new vulnerabilities and operational risks, along with ethical concerns about autonomous systems. Job cuts might make financial sense, but create reputational risks, while over-reliance can create crises when there is a shortage of human capital.

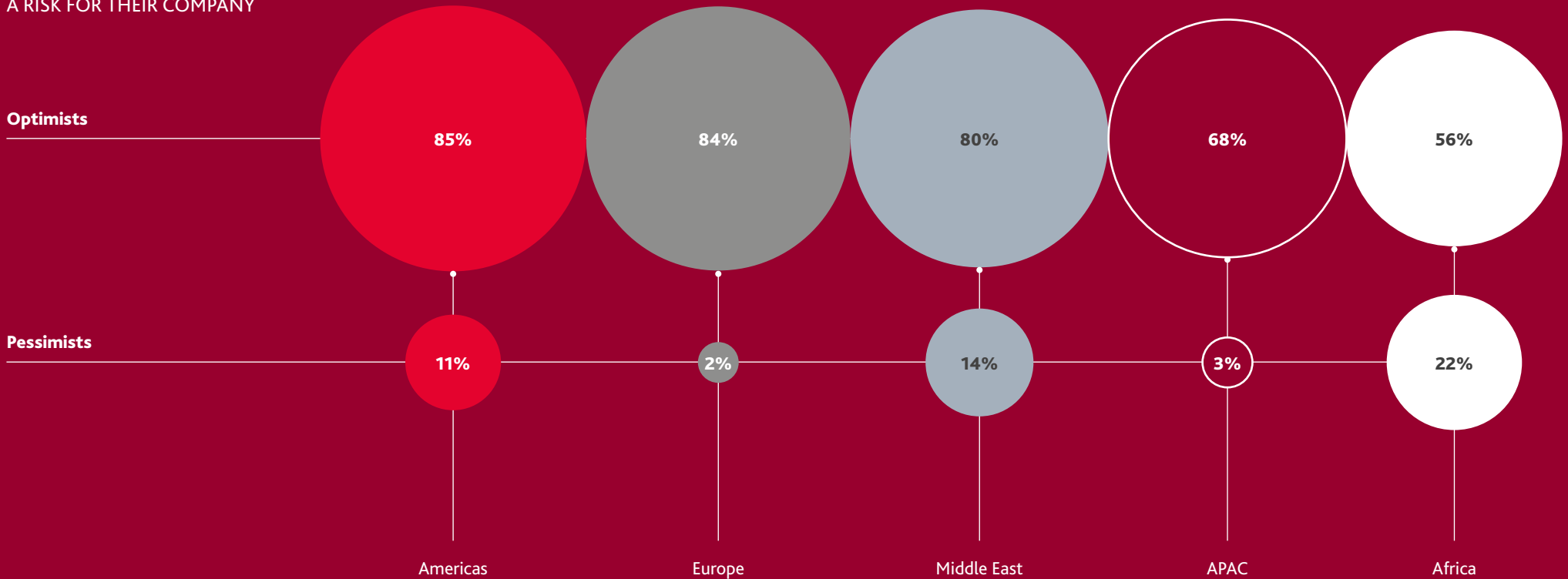
However, the Global Risk Landscape survey shows that business leaders are largely positive about AI, viewing the technology as an opportunity to streamline operations, reduce overhead costs, make fast decisions and facilitate complex tasks, such as wider business strategy.

Simultaneously, 24% of survey respondents consider AI a "significant or somewhat significant" business risk, while 83% consider AI to be a "significant or somewhat significant" opportunity. AI optimists outnumber pessimists by a ratio of five to one.

This view is consistent with a risk-welcoming approach where AI is recognised as a risk multiplier and cyber security issues are likely, but strategies and processes are in place to mitigate new risks. The main challenges associated with digital transformation, which increasingly involves AI solutions, are compliance with data protection and privacy laws (24%) and protecting systems from cyberattack (23%).

Cyber security is a high priority globally, with 74% of all respondents saying that cyber security is the number-one risk priority for their organisation and 55% are struggling to handle the speed and sophistication of current cyberattacks. A worthwhile strategy could be to include AI risks in an organisation's continuous risk assessment process to evaluate the different potential impacts that the use of generative AI may have on businesses.

EXECUTIVES SEEING AI AS
A RISK FOR THEIR COMPANY



Glenn Pomerantz, Forensic Partner and Global Forensic Leader, BDO USA, says that while criminals use AI, the technology is useful for mitigating risks, such as cyberattacks and fraudulent activities: “You can mitigate, you can deter and you can be very careful about who you deal with, whether it’s a business partner, an agent, a distributor, an employee or a counterparty, but ultimately it comes down to early detection,” he says.

“A lot of that is analytics-driven — do you have the analytics or AI in place to detect anomalies quickly and get them investigated immediately? — and most companies don’t, so they’re happy to use those analytics or hire someone to use them after the fact.”



DO YOU HAVE THE ANALYTICS OR AI IN PLACE TO DETECT ANOMALIES QUICKLY AND GET THEM INVESTIGATED IMMEDIATELY?

GLENN POMERANTZ
Forensic Partner and Global Forensic Leader, BDO USA

CONCLUSIONS

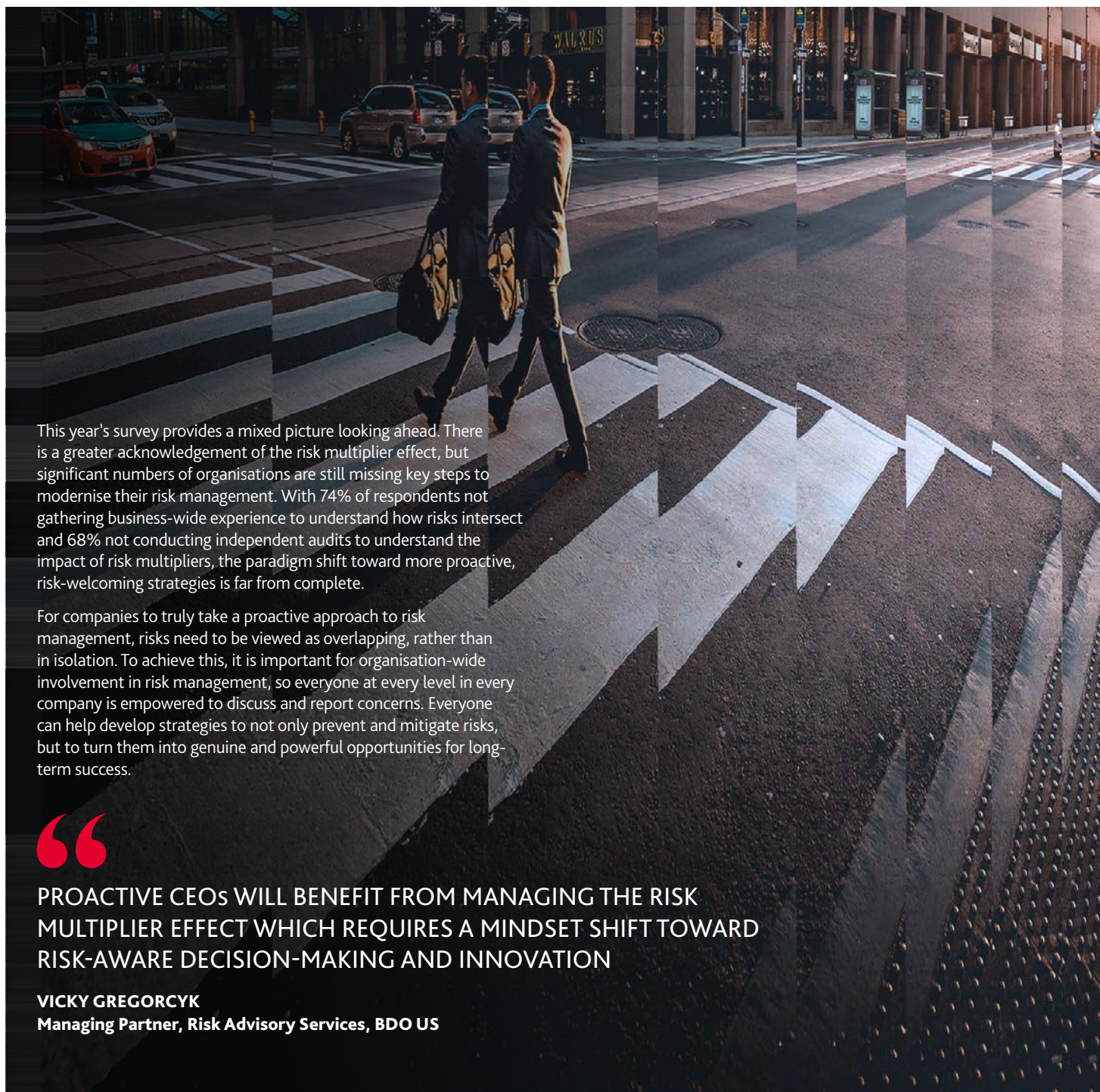
INTERSECTING RISKS ARE HERE TO STAY

The risk multiplier effect is widely recognised across industries and markets. Our 2023 Global Risk Landscape survey showed that 78% of respondents say the global risk landscape is best characterised by the connections between risks, rather than the risks themselves. But not all organisations are moving toward a risk-welcoming approach, where risks are viewed as opportunities for improvement and resilience, rather than threats to be avoided at all costs.

Cyber security risks remain a high priority, but when it comes to fraud, a common risk multiplier with cyber, there is a reluctance to allow independent auditors to provide objective third-party assessment. Companies that do not involve senior leadership in fraud prevention, and cyber crime prevention overall, will struggle to manage this threat effectively.

The widespread use of generative AI technology, as a way to improve business operations for online crime, further amplifies cyber-risks and demands. Companies will need to find a balance between managing risks proactively and reaping AI's benefits.

ESG considerations intersect with many threats, particularly climate and human capital risks. Despite this increasing complexity, many businesses still manage such risks based on regulatory compliance, rather than taking strategic, proactive steps to turn threats into opportunities and mitigate unavoidable risks. While there is greater acknowledgement of climate risks than there was a year ago, 62% of respondents were more interested in meeting regulatory targets than business protection.



This year's survey provides a mixed picture looking ahead. There is a greater acknowledgement of the risk multiplier effect, but significant numbers of organisations are still missing key steps to modernise their risk management. With 74% of respondents not gathering business-wide experience to understand how risks intersect and 68% not conducting independent audits to understand the impact of risk multipliers, the paradigm shift toward more proactive, risk-welcoming strategies is far from complete.

For companies to truly take a proactive approach to risk management, risks need to be viewed as overlapping, rather than in isolation. To achieve this, it is important for organisation-wide involvement in risk management, so everyone at every level in every company is empowered to discuss and report concerns. Everyone can help develop strategies to not only prevent and mitigate risks, but to turn them into genuine and powerful opportunities for long-term success.



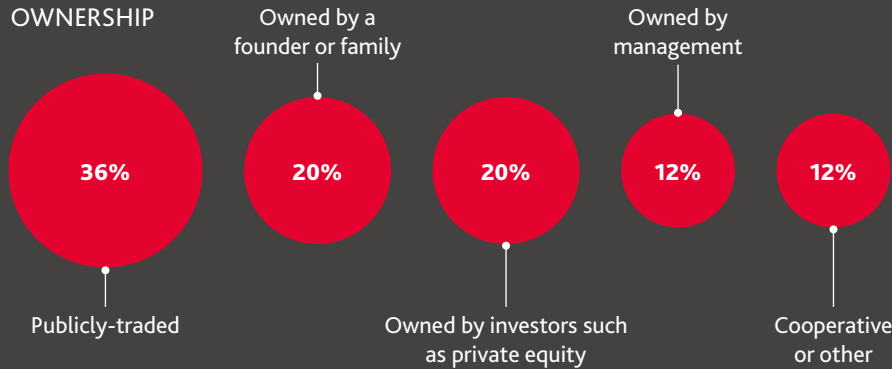
PROACTIVE CEOS WILL BENEFIT FROM MANAGING THE RISK MULTIPLIER EFFECT WHICH REQUIRES A MINDSET SHIFT TOWARD RISK-AWARE DECISION-MAKING AND INNOVATION

VICKY GREGORCYK
Managing Partner, Risk Advisory Services, BDO US

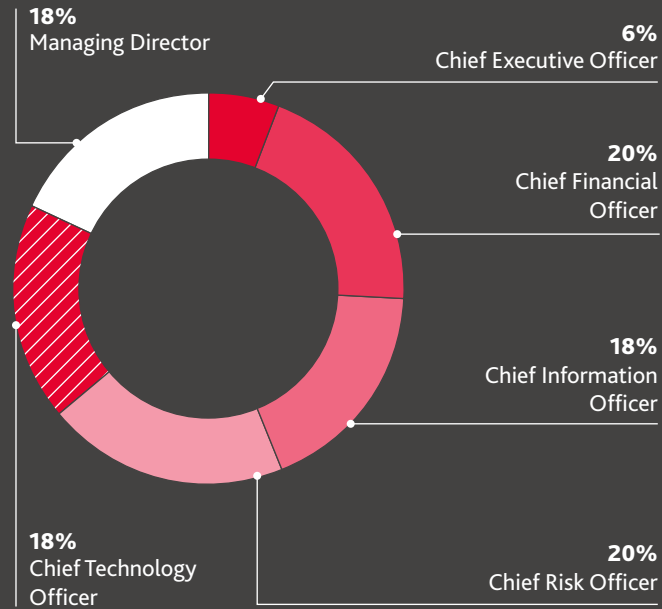
DEMOGRAPHICS AND METHODOLOGY

A BREAKDOWN OF THE BUSINESS LEADERS SURVEYED FOR THIS YEAR'S REPORT

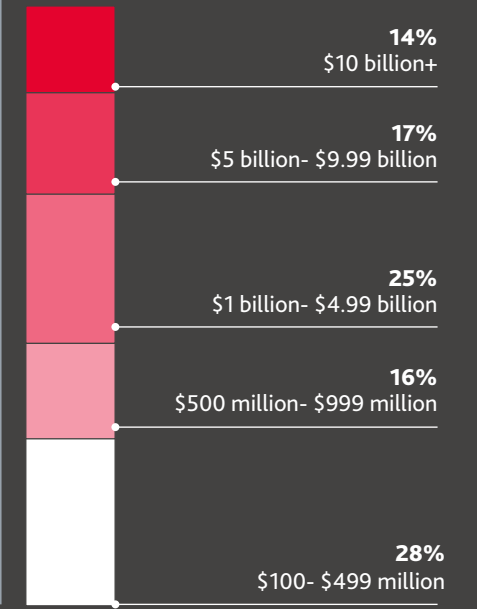
TOP-LEVEL OWNERSHIP



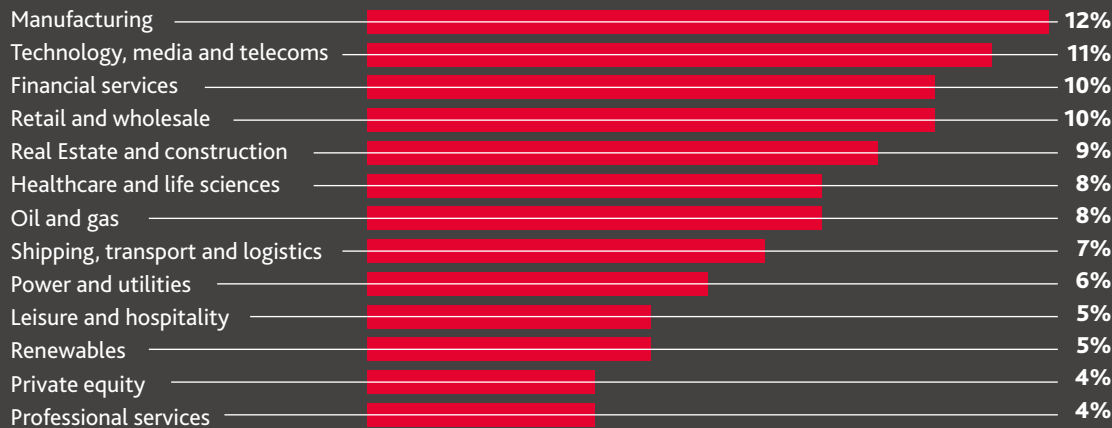
JOB TITLE



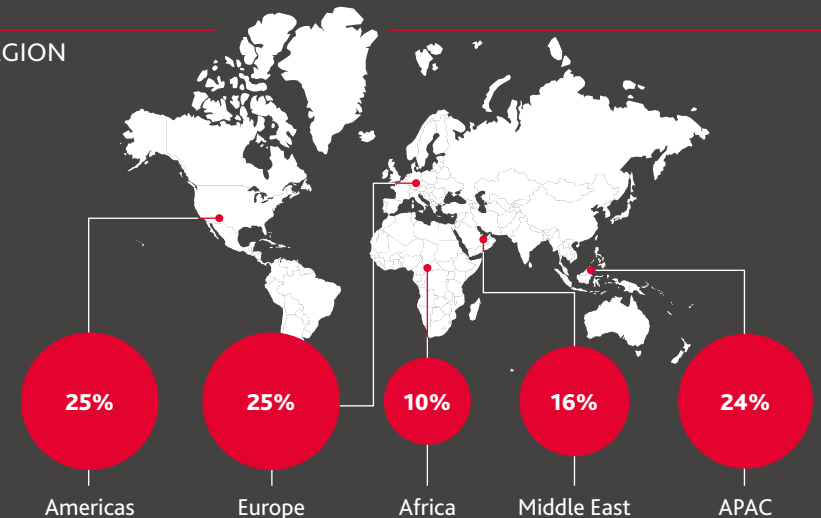
ANNUAL REVENUE



SECTOR



REGION



FOR MORE INFORMATION:

NIGEL BURBIDGE

+44(0)7802 755021
nigel.burbidge@bdo.co.uk

Service provision within the international BDO network of independent member firms ('the BDO network') is coordinated by Brussels Worldwide Services BVBA, a limited liability company incorporated in Belgium.

Each of BDO International Limited (the governing entity of the BDO network), Brussels Worldwide Services BVBA and the member firms is a separate legal entity and has no liability for another such 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 BVBA and/or the member firms of the BDO network.

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

www.bdo.co.uk

