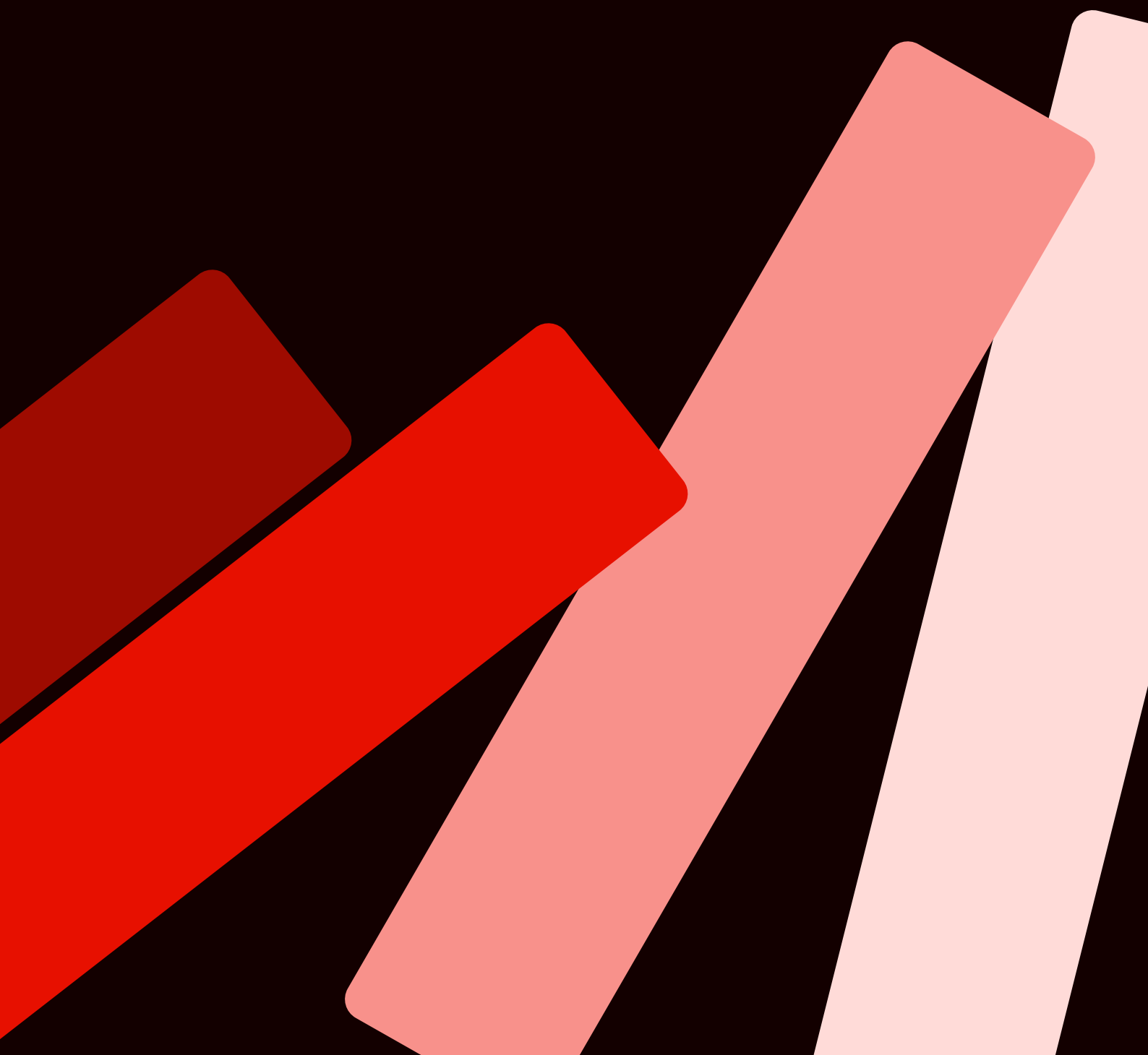


Global Risk Report 2026

Risk in motion



Today's risks are increasingly interconnected. What begins as a single event can quickly trigger a chain reaction across an organisation.



Kate Markham
Chief Executive Officer
Hiscox London Market

AI-enabled fraud, for example, may lead to a cyber attack or wider technology disruption. Economic stress can increase workforce instability and heighten geopolitical tensions, while natural catastrophes can trigger disruption across multiple areas. As technical, financial and operational systems become more interconnected, disruption spreads faster and hits harder, making preparedness ever more challenging.

New research from Hiscox, based on a global survey of 800 risk managers at multinational organisations in eight regions shows the strength and direction of increasingly connected risks. More than half of risk managers regularly experience multiple risks at the same time, and nearly all believe their organisations still underestimate how quickly one event can trigger another.

The findings challenge how risk is typically discussed and managed. Many risk management frameworks continue to treat threats independently – ranking cyber, climate, economic and geopolitical risks as separate issues. In practice, risk is a system. Insurance therefore has a critical role to play, not simply in providing financial protection after a loss, but in helping organisations build resilience and manage interconnected risks before disruption occurs. Today's threats must be evaluated not only by the discrete dangers they pose, but also by what risks they trigger elsewhere and what actions are already in motion – perhaps unseen. Business resilience and insurability must be built in earlier, not left for when it is too late.

Our research reveals the degree to which different risks are connected. Cyber risk emerges with the most connections and the strongest effects on other risks. This includes strong ties to AI-enabled fraud, an accelerant for tech-borne risk across organisations. Beyond wreaking havoc for a business, our research found that cyber threats can lead to a host of other risks: economic, workforce, global relations and deteriorating trust in institutions.

By comparison, some risks that get a lot of attention, like natural catastrophes, have weaker impacts on other threats and are not as central in driving knock-on effects. The findings are critical to informing risk response models and threat assessments.

The research also reveals a growing gap between investment and capability. Organisations are allocating more resources to risk management. But fewer than half of risk managers believe current models capture interconnected risks well. Looking ahead, emerging and frontier risks will add further complexity. The implication is clear. Managing risks event-by-event is no longer sufficient. Resilience now depends on understanding how risks interact and how disruption spreads. Organisations that treat risk as a connected system will be far better placed to navigate uncertainty with confidence.

Executive summary

A new era of risk

The message from risk managers is clear: risks are becoming more connected, more complex and harder to contain. From cyber threats and AI-enabled fraud to emerging technology risks, the findings reveal a growing gap between how risk behaves and how organisations are structured to manage it.

Surveyed risk scenarios

Cyber threat; economic downturn; geopolitical fragmentation and conflict; workforce instability; AI-enabled fraud; digital infrastructure fragmentation; social polarisation and declining institutional trust; climate policy shifts; sovereign debt crises; natural catastrophe events.

51%

of risk managers experience multiple interconnected risks simultaneously.



65%

believe risks are more interconnected than five years ago.



94%

believe organisations underestimate cascading risk impacts.



27%

say one risk event regularly triggers another.



55%

identify cyber threats and AI-enabled fraud as the strongest risk combination.



69%

expect risk management investment to increase in the next year.



84%

believe siloed business units slow response rates to interconnected risks.



50%

struggle to coordinate across teams when managing interconnected risks.



42%

cite regulatory uncertainty around technology as a top emerging risk.



Risk spreads as a system

No risk exists in isolation

Increasingly, risks move through organisations as connected components of an irregular but integrated system. Disruption in one area can quickly trigger pressure elsewhere. This shift is a fundamental change in how organisations experience risk, and how they prepare to prevent them. More than half of risk managers (51%) regularly experience multiple interconnected risks at the same time, while 27% report that one event frequently triggers another.

The resilience challenge

Risk managers see this more often now. Nearly two-thirds (65%) believe risks are more interconnected than they were five years ago, particularly in major markets such as the UK (76%) and the USA (72%). Yet despite this shift, 94% of risk managers believe organisations still underestimate the impacts of cascading risks, which is an initial threat or failure triggering a chain reaction that escalates across the business, industries or economies.

As risks become more interconnected, organisations need a broader view of resilience that considers how disruption spreads across operations, people and technology.

For insurers and brokers, understanding these connections is becoming increasingly important when assessing exposure, strengthening resilience and supporting long-term insurability.

When risks collide

Too many organisations are still not structured to respond effectively to this interconnected system of risk. For half of risk managers (50%), the biggest challenge when multiple risks emerge simultaneously is coordinating across teams, functions or insurance policies. Almost as many (46%) struggle to determine where one issue ends, and another begins.

For risk professionals and insurers, this means evaluating threats not only by their individual severity, but by their ability to trigger wider disruption across an organisation. Understanding these pathways is becoming increasingly important for effective risk financing, resilience planning and underwriting.

Disruption scenarios

Risk managers face two forms of disruption: compounding and recurring. Compounding disruption occurs when interconnected threats emerge simultaneously, while recurring disruption involves repeated versions of the same event. Most risk managers (56%) consider compounding threats to be more disruptive, while 44% are more concerned by recurring disruption.

Regional differences are evident. Risk managers in Germany (52%) and the Nordic countries (51%) are more likely to view recurring disruption as the greater challenge than those in the USA, Canada, the UK, France and Australia, while opinion in Japan is evenly split.

Recurring disruption



Compounding disruption



Balanced view



The connected risk network

The central role of cyber

To understand how modern business disruption spreads, look to cyber threats. As a risk, it is central to the system because it connects to, amplifies and is affected by the most risks.

Cyber threats have the strongest connection to AI-enabled fraud. Together, they create one of the most powerful transmission pathways across the wider risk system and should increasingly be thought of together.

Unlike natural catastrophes, cyber risk is not entirely beyond an organisation's control. Businesses can take meaningful steps to reduce both the likelihood and impact of an attack, making it a threat that is not only worth combating but essential to monitor closely. It's a risk that regularly causes other risks to arise, but also organisations can exact a degree

of control over mitigating this, which is all but impossible with natural catastrophes or broader economic forces.

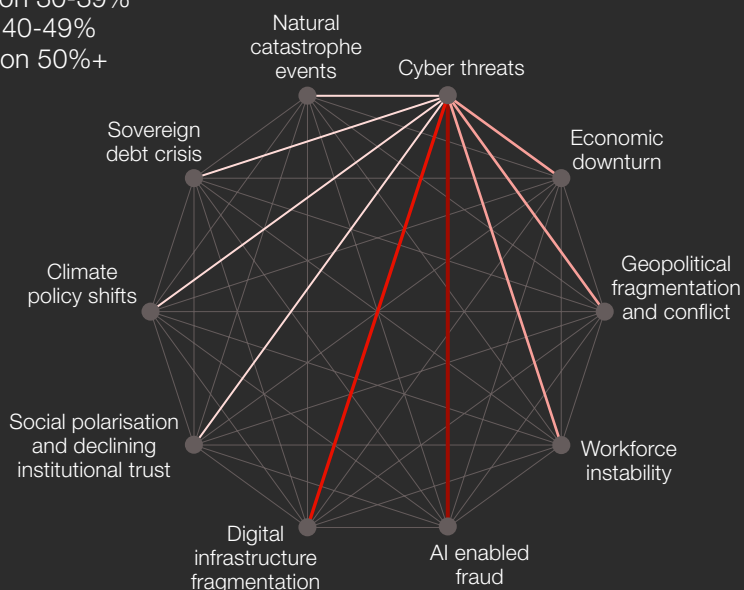
Rather than a discrete technical crisis, cyber risk is increasingly embedded within broader organisational instability. For example, cyber threats can drive a breakdown of critical digital systems. Other times cyber threats can be a follow effect of global political instability and conflict.

Organisations should think less about isolated cyber events and more about cyber as a catalyst within a wider risk system. As digital dependency grows, cyber resilience increasingly underpins resilience across multiple business functions, from operations and workforce stability to financial performance and stakeholder trust.

Cyber threats

With strong links to AI-enabled fraud, cyber threats frequently trigger wider organisational disruption. Unlike many other systemic risks, they can be mitigated through robust controls and preparedness, making them critical to track and address.

- Weak connection <30%
- Moderate connection 30-39%
- Strong connection 40-49%
- Strongest connection 50%+



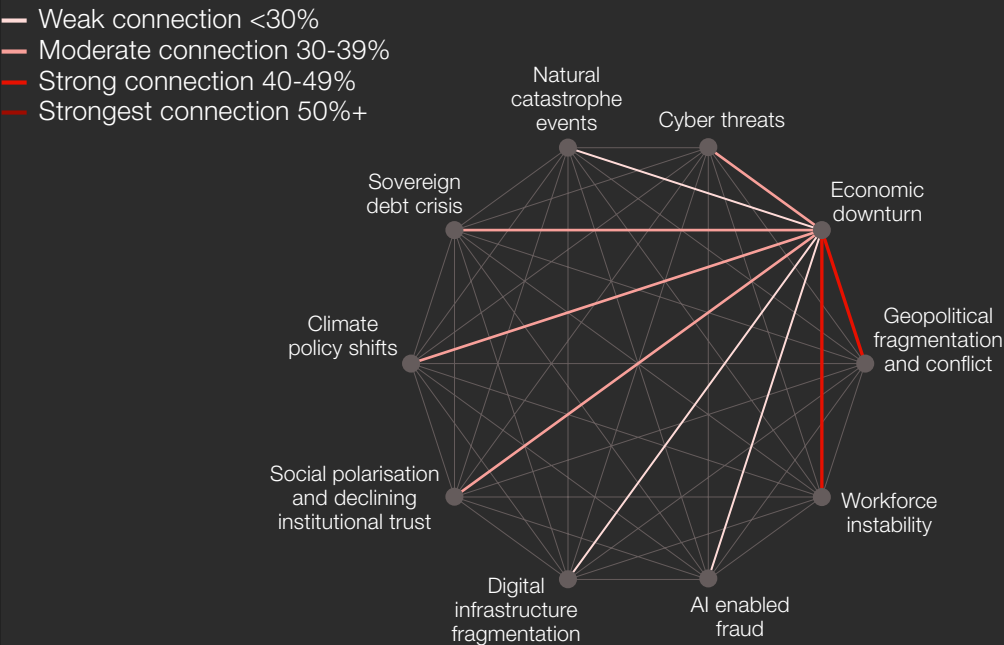
The connected risk network continued

Other disruption drivers

While cyber threats are the most connected risk in the system, they are not the only ones that influence how disruption unfolds. Many other risks also play important roles in transmitting and amplifying disruption across the network.

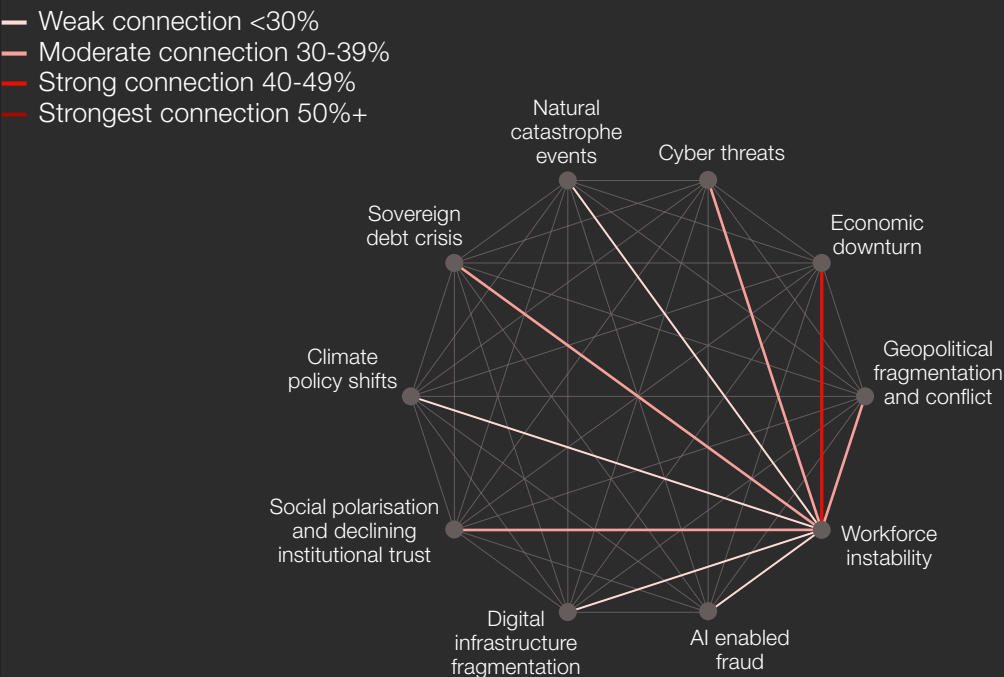
Economic downturn

Our research reinforces the strong link between challenging economic conditions and workforce instability. It also shows that instability can emerge from geopolitical shifts, cyber threats and changes in climate policy.



Workforce instability

In the modern risk system, workforce instability largely follows other pressures, particularly economic disruption and geopolitical fragmentation.

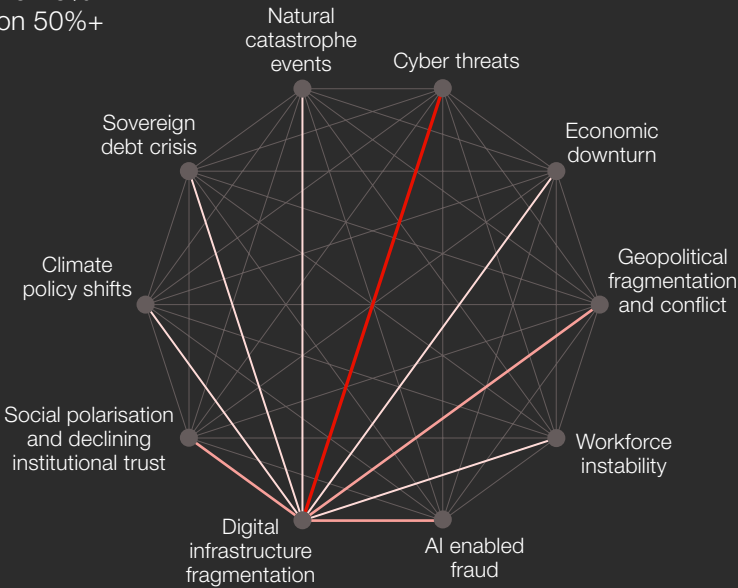


The connected risk network continued

Digital infrastructure fragmentation

Cyber threats and AI-enabled fraud are increasingly acting as catalysts for wider disruption across critical digital systems and networks.

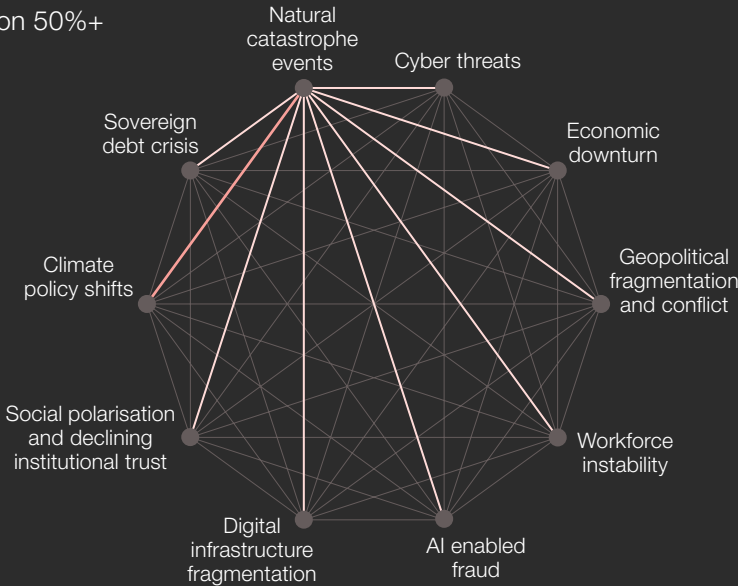
- Weak connection <30%
- Moderate connection 30-39%
- Strong connection 40-49%
- Strongest connection 50%+



Natural catastrophe events

While natural catastrophes dominate headlines, they are less connected with weaker bonds to other threats.

- Weak connection <30%
- Moderate connection 30-39%
- Strong connection 40-49%
- Strongest connection 50%+



The connected risk network continued

Adapting to interconnected risk

While risk managers globally recognise growing interconnectedness, confidence in preparedness varies significantly across markets. Risk managers in France (28%) and the Nordic countries (24%) are much more likely to think their risk models perform poorly on identifying interconnected risks compared with Australia (5%), the USA (7%) and Germany (15%).

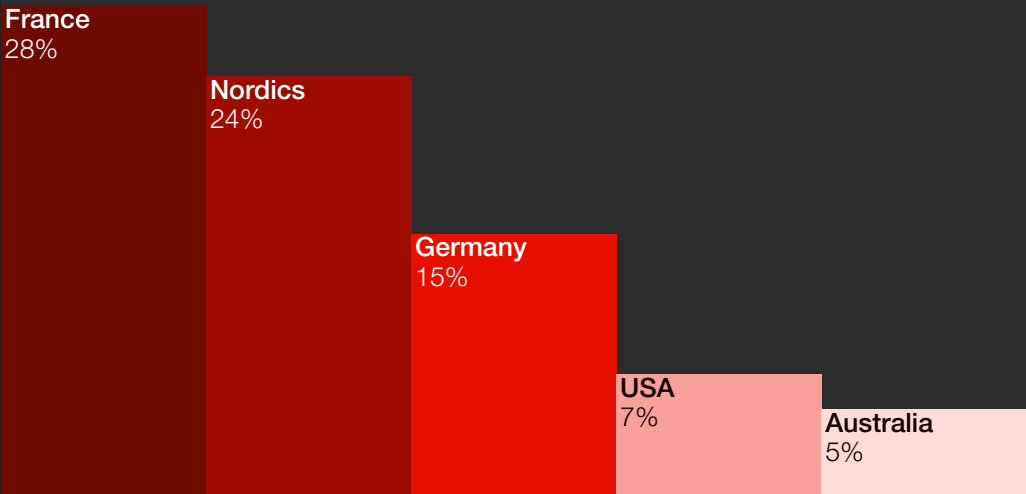
Perceptions of organisational preparedness also differ. While a majority of risk managers in every region believe their organisations underestimate cascading risks, this view is less pronounced in Australia (83%) than in Canada and Japan (97% each), the USA (99%), Germany (95%), and France and the Nordics (both 94%).

Investment expectations vary sharply as well. More than four-in-five risk managers in Australia (84%) and the USA (83%) expect investment in risk management to increase over the next year, compared with 64% in Germany and Japan and just 44% in the Nordic countries.

The differences in preparedness suggest organisations are at varying stages of adapting to a more interconnected risk environment. The next challenge is ensuring investment and organisational capability keep pace with the changing nature of risk.

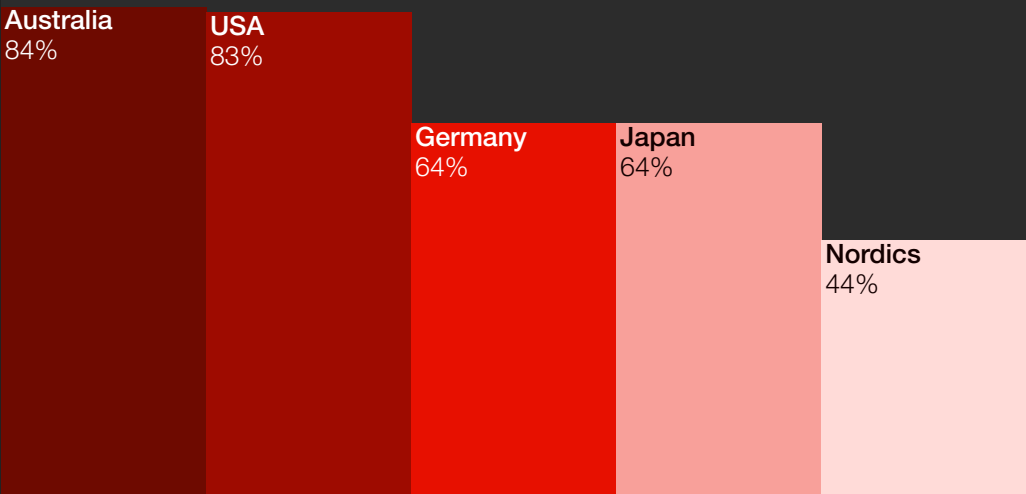
Confidence in risk models

Percentage of risk managers who believe their risk models perform poorly on identifying interconnected risks.



Investment expectations

Percentage of risk managers who expect investment in risk management to increase over the next year.



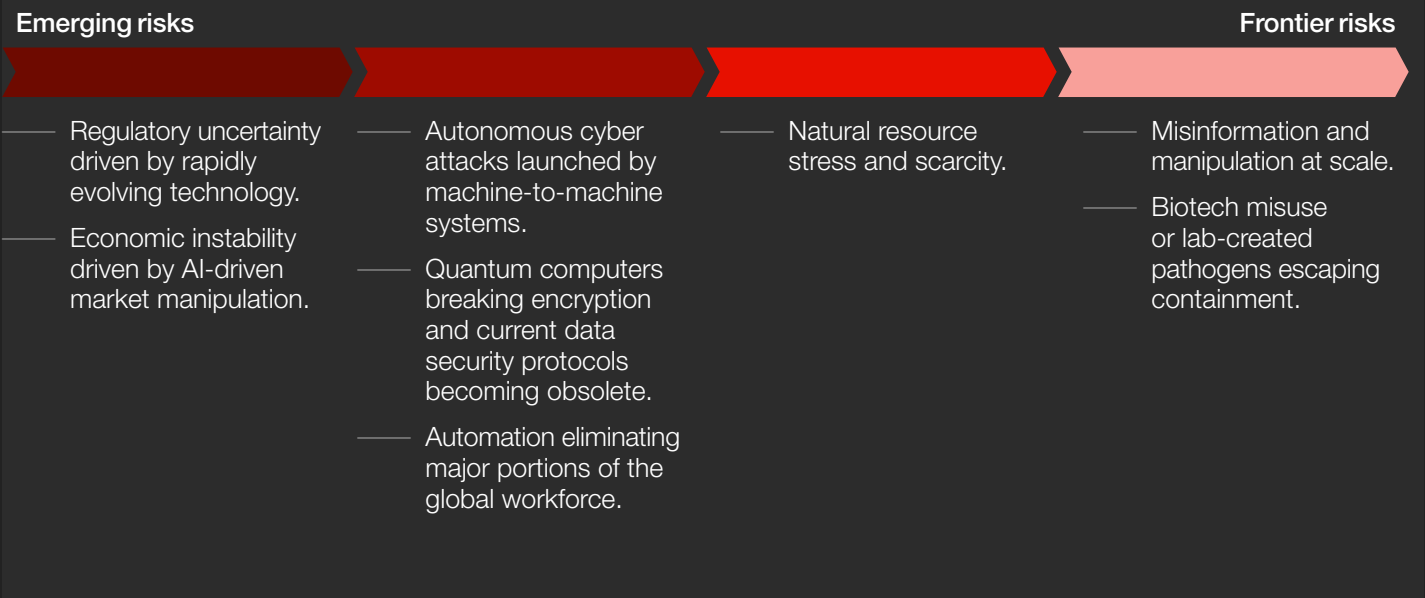
The network keeps growing

Tomorrow's interconnected risks

Looking ahead, emerging and frontier risks will add further complexity. Emerging and frontier risks sit at different points on the spectrum of uncertainty. Emerging risks are evident but still developing or rapidly evolving, with uncertain impact, timing and consequences and limited historical data to support modelling. Frontier risks exist at the outer edge of current understanding, operating in a largely pre-regulatory, pre-legal landscape with little historical precedent. As a result, organisations may struggle to define credible scenarios or develop effective mitigation approaches.

The changing risk landscape

Consider these scenarios, progressing from emerging threats to those at the frontier of current understanding.



Key takeaways

Investment in risk management is rising

What the data shows

- 69% of risk managers expect spending to rise over the next 12 months, 19% expect no change.
- Economic uncertainty (41%) is the leading driver, followed by resilience, emerging technology risks and regulatory change (40% each).

Why it matters

- Organisations are increasingly viewing resilience as a strategic investment rather than a cost. Rising investment reflects growing recognition that traditional approaches are no longer sufficient, with businesses prioritising preparedness, visibility and resilience.

The resilience paradox

What the data shows

- Investment in risk management is rising, but confidence is not. Fewer than half (48%) of risk managers believe their current models capture interconnected risks very or extremely well.

Why it matters

- Despite increased investment, risk management capabilities are struggling to keep pace. Many organisations remain unsure whether their models can capture interconnected risks. Closing the gap between spending and risk intelligence will be critical to anticipating disruption and strengthening resilience.

Risk remains siloed

What the data shows

- 39% of risk managers categorise risks by impact, while just 26% organise them around how threats interact.
- 50% say coordination is the biggest challenge, with 84% saying silos slow response during interconnected disruption.

Why it matters

- The greatest vulnerability may be organisational rather than technical. Silos slow decision making and hinder responses when multiple threats emerge. The organisations that improve cross-functional collaboration will be better positioned to respond quickly and build resilience.

Visibility doesn't equal influence

What the data shows

- Natural catastrophes may dominate headlines, but are less likely to be drivers of wider disruption. Economic downturns and cyber threats are more likely to influence and amplify risks across the wider risk ecosystem.

Why it matters

- The most visible risks are not always the most influential; with some acting as catalysts that amplify disruption across organisations and the wider economy. Risks should be assessed not only by their severity, but also by their potential to trigger, connect or accelerate other threats.

Mind the investment gap

What the data shows

- Economic uncertainty (42%) is the leading factor preventing organisations from increasing investment in risk management.
- Investment is also suppressed by competing leadership priorities (38%), perceptions that risks remain stable (37%), and expectations that AI can absorb workloads (35%).

Why it matters

- Budget constraints and competing priorities continue to limit investment in risk capabilities, despite a more connected and complex risk landscape. Organisations that delay investment risk widening the gap between emerging threats and their ability to anticipate, withstand and respond effectively.

Hiscox

22 Bishopsgate
London EC2N 4BQ
United Kingdom

+44 (0)20 7448 6000
enquiries@hiscox.com
hiscoxlondonmarket.com

Report methodology

The survey was conducted by Wakefield Research among 800 risk managers at multinational companies in the following markets: Australia, Canada, Denmark, Finland, France, Germany, Japan, Norway, Sweden, UK and USA, between February 20 and March 3, 2026, using an email invitation and an online survey. Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. For the interviews conducted in this particular study, the chances are 95-in-100 that a survey result does not vary, plus or minus, by more than 3.5 percentage points in the total sample, and 9.8 percentage points in each market from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

HSXSB441