MARSH

Fifth edition

UK business risk report

Surveying the business risk landscape through the views of 2,000-plus business leaders.

Contents

Foreword from the CBI

For businesses up and down the country, “risk” is no longer defined by isolated shocks, but by an interconnected landscape that is reshaping the environment in which UK businesses operate.

Uncertainty has shifted from being a temporary condition to a structural feature of the business landscape. UK businesses are confronting a complex environment shaped by geopolitical instability, rapid technological change, supply chain fragmentation, and climate pressures. The shocks of recent years, from the pandemic, global conflicts, to supply chain disruption, have underscored the necessity for robust and adaptive systems capable of withstanding, responding to, and recovering from crises.

This year's *UK Business Risk Report* highlights a clear shift in boardroom priorities. For the first time, cyber risk ranks as the leading concern for business leaders. High-profile attacks, rising costs, and vulnerabilities embedded in supply chains have moved cybersecurity to the centre of corporate strategy. But cyber risk is not isolated; it cuts across economic, financial, and people risks, including skills, leadership, and governance. Climate risk too is evolving. Once viewed primarily through the prism of flooding, it now encompasses heat and drought, showing that resilience is no longer a narrow scope.

The biggest feature of today's risk environment is that everything is connected. A cyber incident can trigger financial loss, regulatory scrutiny and reputational damage. Economic volatility can weaken supply chains and constrain investment. Of the 47 risks examined in this research, the overwhelming majority are cited as material. However, different sectors and types of businesses see risks differently, which leads to gaps and inconsistencies in how they plan for resilience.

The CBI has consistently argued that growth and resilience are two sides of the same coin. When governments provide strategy and vision, businesses can turn it into action through their expertise, investment, and innovation. But clarity is essential. A shared definition of resilience, aligned across government, regulators, and industry, is crucial if we are to build traction and momentum. What resilience means for society is not always the same as what it means for an individual firm.

Resilience is also what can set businesses apart. Those that invest in it are better equipped to manage uncertainty and deliver long-term growth. Encouraging private sector investment in resilience must now be a priority, which means tackling the barriers that hold firms back, including skills shortages, limited access to finance, and difficulties in assessing risk.

In the rapidly shifting international risk environment where risks cascade and compound, resilience is not an add-on. It is a core component of long-term competitiveness. By strengthening partnership between business and government, the UK can build the resilience needed not only to withstand disruption, but to drive growth.

John Foster, Chief Policy and Campaigns Officer, CBI

Executive summary

Complex risk driving pivot to flexible, streamlined resilience

Interconnected, interdependent risk highlights the importance of expert support and advice

This year's *UK Business Risk Report* finds business leaders operating in a fluctuating macroeconomic environment — with easing inflation, lower interest rates, and steadier energy prices — but facing persistent threats from cybercrime, political turbulence, and extreme weather. For the first time, cyber risk is the top concern, driven by high-profile attacks, rising incident costs, and cyber risks originating in third-party suppliers. Nearly half of UK businesses identify cybercrime as a real worry.

A defining theme is interconnectivity: risks are now a complex web in which incidents in one area (people, supply chain, compliance) can cause cyber incidents, and cyber events can cascade into financial and regulatory consequences and brand and reputational damage. A further sign of real worry about the broad array of risks facing businesses is that almost half cite "brand damage" — so often a consequence of incidents in other risk areas — as a real concern. What's more, of 47 specific risks across eight categories

we asked businesses about, 36 were cited by at least one in five business leaders. Indeed, more than 90% pointed to at least one risk of concern across every category — from cyber and economic risk to people and environmental risk.

In response, businesses have made targeted investments over the last 12 months to manage "trigger" risks — those whose impact fans out across multiple areas. Reviewing cybersecurity controls is now among the top five risk actions; significant attention is also directed at people and supply chain risk.

Perhaps the clearest sign that business leaders recognise they are operating in a diverse web of risk and are responding with purpose lies in their ambitions to use tools and technology to build streamlined, adaptable risk management capabilities.

More than 70% of firms plan to adopt technologies such as learning and training platforms, cybersecurity solutions, risk management software, data analytics, and Internet of Things, to build streamlined, adaptable risk capabilities and to simplify insurance administration.

While the shift to targeted, tech-enabled, agile risk management is encouraging, fewer businesses now have firm plans for future resilience investment than in the previous year. This underscores cautious optimism tempered by the need for proactive horizon scanning and independent expert guidance to build the flexible, streamlined resilience required in an interconnected risk landscape.

Once again, this highlights the importance of seeking independent support and guidance from experts with broad risk expertise. Advice of this type can help businesses take more targeted and agile approaches to risk management — from property and people to leadership, environmental, and cyber risks. Crucially, it can also help businesses navigate emerging challenges — from anticipating new threats to preparing for the future by building the streamlined, flexible, agile risk management capabilities they need to thrive in an uncertain risk environment. If you would like to discuss any of the risks identified in this report in more detail, please contact your Marsh advisor.

Alistair Brighton, CEO, Corporate & Commercial, Marsh UK

Key takeaways:

- Review your internal and third-party cybersecurity policies and procedures — here are 12 key cyber controls you can set up right now.
- Risk management initiatives should be equal to the sales strategy or client experience programme — seek independent expert guidance to build resilience.
- Enhance employee engagement by leveraging benefits technology platforms — no longer limited to larger firms, these are now widely available.

Risks ranked

Navigating choppy waters

The key risks cited by business leaders

46%

Cyber risk (for example, cybercrime, and IT network and service disruptions)

44%

Economic and financial risk (for example, inflation, recession, cash flow, currency, and credit risk)

40%

Compliance, legal, and regulatory risks (for example, new rules, legislation, trade tariffs, employment law, and customs)

39%

People risks (for example, talent acquisition and retention, mental health and wellbeing, culture, and health and safety)

36%

Operational and supply chain risk (for example, equipment breakdown or theft, logistics, and failure of key suppliers or customers)

34%

Strategic and reputational risk (for example, new competitor, damage to brand and image, consumer behaviour)

31%

Environmental risks (for example, net zero, natural disasters, or other extreme weather-related risks)

This year's report sees UK businesses continuing to navigate a complex array of risks. Indeed, while the fourth edition of this report (2024) identified business leaders increasingly dealing with interconnected risks, this year, that complexity appears to be viewed as a "new normal," in which a web of interrelated risks constantly shifts and evolves as external events ebb and flow.

Cyber is now the number one risk

The rise of cyber risk, an inherently interconnected risk, is the most striking finding. Having been a peripheral risk in the minds of business leaders a few short years ago, cyber has continued a precipitous climb, now standing as the number one risk category facing UK businesses.

Almost half (46%) pointed to cyber risk as a priority risk category this year, compared with 39% in 2024. It is not hard to understand why, with 2025 having brought a rash of high-profile and highly disruptive cyberattacks affecting UK household names.

A bumpy ride

The rise of cyber may have knocked economic and financial risk, seemingly ever-present, off the top spot, but this does not mean concerns in this area are receding. In fact, issues like inflation, interest rates, energy prices, and macroeconomic turbulence are now a concern for 44% of business leaders, up 1 percentage point from 2024.

This may reflect what has undeniably been a bumpy 18 months for the new UK government, which has, to date, been unable to stimulate significant economic growth while raising taxes on businesses through a hike in employers' National Insurance contributions.

Internal risks remain a key concern

Similarly, business leaders are more concerned about compliance and regulatory risks than they were two years ago. Today, 40% point to this category as a key risk, compared with 37% in 2024, a change which has seen compliance and regulatory risk climb to third in the list of key business risks. This may be in anticipation of the full implementation of the Employment Rights Act 2025, as well as a slew of changes to the way the Health and Safety Executive plans to enforce existing regulations.

Finally, another interconnected set of risks, those associated with operational and supply chain issues, is a further cause for concern among business leaders. This year, 36% see this as a key risk area, compared with 34% two years ago. It remains in fifth place overall behind people risks, which fell to fourth place, despite a slight rise in the percentage of business leaders seeing it as a key risk (39%, versus 38% in 2024).

A complex web of risk

It is interesting to note that the overall proportion of business leaders citing each of the top five risk categories above as a concern has risen slightly, even though some positions in the top five have changed.

This, coupled with the fact that the top five risks are all cited by between 46% and 36% of business leaders, again points to the sheer complexity of the risk environment in which UK firms are now operating. No one risk dominates, and all can be characterised as being of real concern.

As we will see in the following chapters, this complex, heightened risk landscape is only rendered more difficult to navigate by the interaction between risks and the sheer pace of change. We will also look in detail at how business leaders are responding, their plans to further invest in risk management, how they are using technology to evolve and adapt to the "new normal," and signpost some of the solutions businesses could employ in this age of a complex, ever–changing web of risk.

Cyber risks

Which cyber risks to your business, if any, concern you most?

1. Cybercrime, (for example, ransomware, phishing, and deepfakes)

44%

2. Service disruptions (for example, from third–party provider)

33%

3. Digital transformation (for example, adoption of emerging technologies, including AI and ChatGPT)

29%

4. Internal IT network disruption

28%

5. Insider threat (for example, employee error)

26%

Businesses are more concerned about cyber risk than ever before, following steadily rising awareness over the last five years. To put that in context, in the 2023 Marsh *UK Business Risk Report*, just 20% of businesses cited cyber as a key risk. As we have seen, three years later, that has risen to 46%, making cyber the single most important risk in the minds of business leaders.

What's more, pointing to the pervasive nature of cyber risk, 96% of businesses say they are concerned about at least one cyber risk.

The detail set out above is telling. The threat of cybercrime is by far the most serious cyber risk according to business leaders, 44% of whom point to ransomware attacks, phishing, and deepfakes as issues of real concern.

It is not hard to understand why, given the scale of attacks we have seen against UK businesses over the last 12 months alone. Indeed, those attacks may also explain why so many businesses see the risk of IT service disruption originating from the supply chain as a serious problem.

For instance, the ransomware attack that shut down UK online stores for over a month last summer, at a cost of £300 million, started with a phishing attack on an outsourced IT contractor.

The attack on a UK car manufacturer was even more serious. A ransomware attack — the result of a supply chain hack that shut down global production — affected 5,000 suppliers and caused losses of at least £1.9 billion. According to the Cyber Monitoring Centre, it was the most economically damaging hack in history. At the same time, government communications suggested that the shutdown left those 5,000 suppliers on the brink of bankruptcy.

On top of these specific, high-profile incidents and more, the average cost of cyber breaches to UK businesses continues to rise. According to the Cybersecurity Breaches Survey, on average, cyberattacks now cost businesses between £7,960 and £12,560.

Multi–faceted risk: From cybercrime to AI

However, while cybercrime grabs the headlines and is clearly the risk of most concern for UK businesses, they are also increasingly aware that this is a multi–faceted risk area. Alongside cybercrime and supply chain cyber risks, more than a quarter of business leaders are also worried about internal IT network disruption (28%) and insider threat (26%).

Interestingly, this year's survey identifies shifting views on the threat posed by AI. While two years ago, 25% of businesses were concerned about the threat presented by emerging technology like AI in and of itself, this year, the focus is more on the risks associated with adopting and using this technology. That is, while no business saw emerging technology as a risk, almost a third (29%) saw significant risk in digital transformation focused on technologies like AI.

This perhaps speaks to the pace of change in AI technology — the sheer speed of adoption, the scale of opportunity, the risk of being left behind, and the risk associated with getting it wrong.

Sector, size, and geographic variations

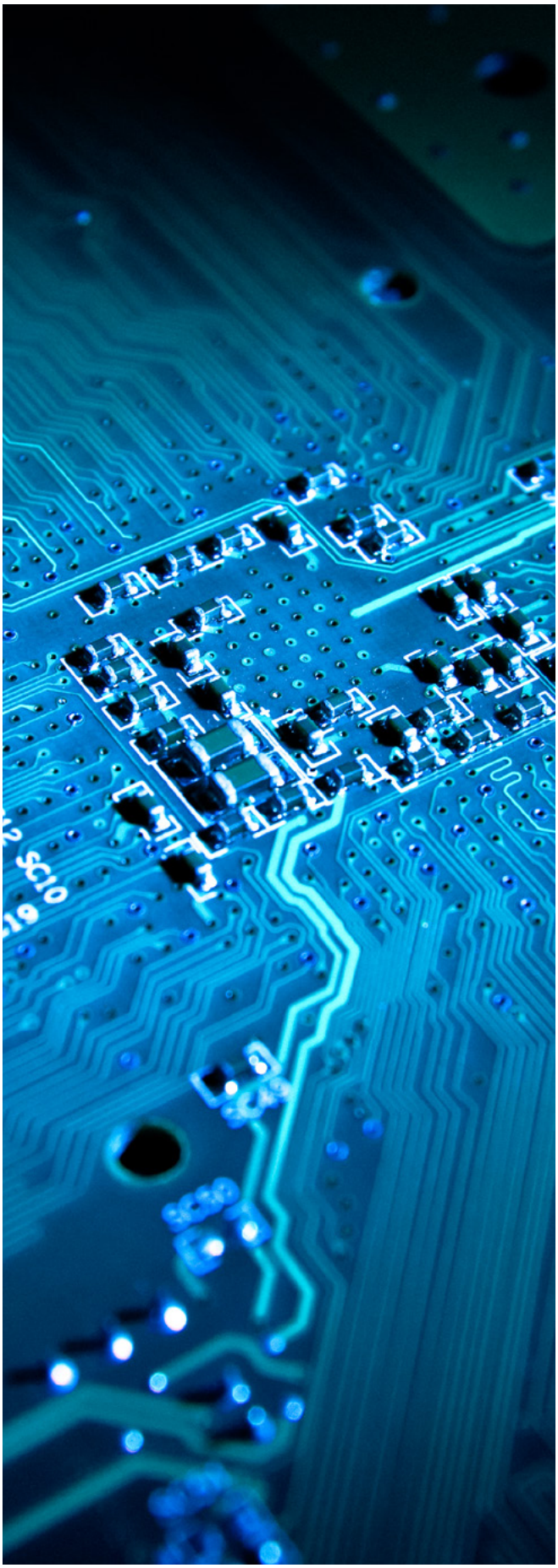
As was the case two years ago, not–for–profit organisations are the most concerned about cybercrime (75%), followed by the renewables (67%) and technology (65%) sectors. Conversely, those in construction, contracting, and engineering (34%), food and beverage sector (35%), and recruitment (35%) sectors are the least worried.

Businesses in the renewables sector are also the most concerned about third-party provider service disruptions (67%), while recruitment businesses are the most worried about digital transformation risks (41%).

Meanwhile, despite the lessons of the UK cyberattacks for small businesses, micro businesses remain the least concerned about cybercrime (36%), compared with 48% of large businesses and 45% of SMEs.

Take action: Businesses concerned about cyber risk can make a start by reviewing their cybersecurity policies and procedures to defend against cybercrime and other risks. Read these 12 controls to help strengthen your cybersecurity to make a start. You may also want to consider accessing expert advice or services such as penetration testing, cybersecurity assessments, GDPR, and cybersecurity training, and data protection officer (DPO) services.

On top of that, given that cyber risk is constantly evolving, many businesses are now turning to cyber insurance, which helps them recover losses and associated costs, for instance, resulting from large–scale breaches, business interruption, ransomware, and other types of cyberattack.



Economic and financial risks

Which economic and financial risks to your business, if any, concern you most?

1. Economic instability in any markets you operate in

30%

2. Risk of recession

25%

3. Inflation risk

22%

4. Cash flow risk

20%

5. Cost of insurance

19%

While at the high level, economic and financial risk remains a serious issue for almost half of UK businesses (44%), the detailed views of UK business leaders tell a different story. No single financial risk comes close to matching that 44%, with concerns around general economic instability rising by five percentage points to emerge as the top risk at 30%.

All other specific finance risks have remained static or fallen in terms of the proportion of UK businesses citing them as a concern, standing at 25% of UK business leaders or fewer. Specifically, the risk of recession is unchanged at 25% of businesses, while inflation risk (22%), cash flow (20%), and cost of insurance (19%) have all fallen.

Risk perception in step with economic reality

In many ways, these figures and the shifting levels of concern over the last two years reflect the economic environment in which businesses are operating. That is, both inflation and interest rates have fallen sharply since their peaks in 2023 and 2024, respectively, with both expected to fall further over the coming year. In turn, this may help to explain why the proportion of business leaders worrying about cash flow has fallen from 25% to 20%.

Meanwhile, although the final quarter of 2025 was marked by widespread fear of a recession, that fear was allayed for the time being when the economy showed weak growth of 0.1% over the period. The fact that recessionary worries have not entirely gone away may explain why risk perceptions in this area remained steady among 25% of business leaders.

Overall, however, 70–80% of businesses are not concerned about these risks, which suggests that leaders feel they are receding, in line with falling inflation and interest rates. In that context, the fact that 44% see economic and financial risk as a key risk, and 30% worry about economic instability, may simply reflect a generalised unease overlaying a slightly more positive outlook overall.

One element in a complex web of risk

All that said, and while no single economic or financial risk is cited by even a third of businesses, it should be remembered that 96% of businesses say that they are concerned about at least one such risk. As we will see throughout this report, these risks are now thoroughly embedded in the business landscape, and part of a complex, diverse, and changing web of risk that business leaders must navigate.

Sector, size, and geographic variations

Businesses in the power and utilities sector are by far the most worried about economic uncertainty, with 60% citing it, twice the average, while those in property or real estate are the least concerned (19%). The power and utilities sector is also the most concerned about cash flow (40%), along with those in the communications and media sector (38%).

Meanwhile, the not–for–profit sector is the most worried about inflation (40%), compared with communications and media, where no businesses cited this as a risk.

On the other hand, concerns around economic and financial risks, insofar as they are perceived at all, stand at broadly similar levels across the UK. At the same time, smaller firms are generally more concerned about cash flow than their larger counterparts (25% of micro businesses, versus 19% of SMEs and 17% of large businesses).

Take action: In a business environment beset by relatively high insolvency rates, businesses can reduce financial uncertainty by defending against non–payment from financially struggling customers. Trade credit insurance can help protect your firm if your customers fail to pay for goods or services provided on a credit basis (where the buyer pays at an agreed future date), usually due to insolvency or a lack of funds.

What's more, this kind of cover can also address interconnected risks — for instance, safeguarding cash flow, while helping to unlock access to debt finance and optimise working capital.

Meanwhile, those struggling with insurance costs can use premium finance solutions to spread payments, typically over 10 to 12 months. This can also protect short-term cash flow and may be deductible from corporation tax.

Business interruption cover can also offer protection for your business and its finances in the event of a serious incident that disrupts your ability to trade normally.

Compliance, legal, and regulatory risks

Which compliance, legal, and regulatory risks to your business, if any, concern you most?

1. Introduction of new rules or legislation

32%

2. Changes to tax/National Insurance

30%

3. Health and safety

29%

4. Employment law

24%

5. Fraud/corruption

23%

As with economic and financial risks, detailed responses around compliance, legal, and regulatory risk tell a more nuanced story than the top-level findings, in which 40% express concern about these risks in a general sense. Again, no single, specific risk matches that level of concern, and, for those where trends can be identified, the level of concern has fallen across the board — even though 97% of businesses say they are worried about at least one compliance risk.

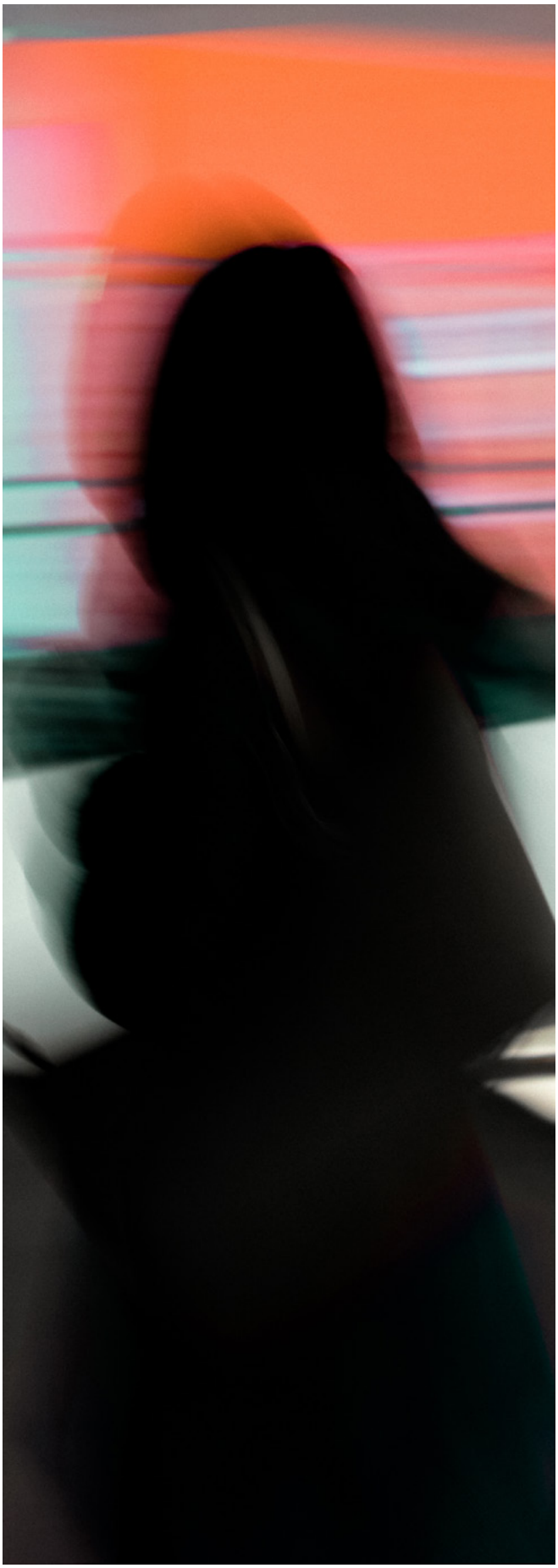
New rules are the biggest concern

Perhaps not surprisingly, with the arrival of a new government since the last Marsh *UK Business Risk Report*, the introduction of new rules or legislation has taken top spot, cited as a worry by 32% of business leaders. However, despite issues such as the Employment Rights Act 2025 passing into law and a change of focus for the HSE, this is less of a concern than it was two years ago (34%).

Similarly, fewer UK business leaders pointed to "traditional" risks in this area than did so two years ago. Health and safety, the top risk in 2024, is down to third place, having fallen by two percentage points. Similarly, a slightly smaller percentage of businesses expresses concern about employment law risks than in 2024 (24% versus 27%).

Trade tariff worries fading?

It is also interesting to note that, despite featuring heavily in the news, trade tariffs are less of a concern than they were two years ago, having fallen out of the top five risks and being cited by 21% of businesses, down from 22%. We can only speculate as to why, but it seems possible that the trade deal signed between the UK and the US in May 2025, and which limited tariffs between the two countries, has played a role here.



Businesses wary of National Insurance rise

One major shift in this area, however, is around "changes to tax and National Insurance (NI)" — almost a third (30%) identified this as a key risk, making it the second most significant compliance and operational concern among business leaders.

Clearly, this is in direct response to changes in government policy, which saw employer contributions rise to 15%, though it is worth noting here that the vast majority (70%) do not consider the change to NI a significant risk.

Sector, size, and geographic variations

It's hardly surprising that concerns differ across sectors, reflecting each industry's distinct priorities. For instance, agriculture (80%) and property and real estate businesses (52%) are most concerned about new rules and legislation, no doubt driven by changes to inheritance tax rules and the Renters Rights Act 2025, respectively.

Communications and media businesses are the most concerned about changes to tax and NI (63%), but among the least concerned about health and safety (13%). In terms of health and safety risks, power and utilities were the most worried (60%).

Finally, smaller businesses are most concerned about new rules and legislation, with 36% of micro businesses citing this as a key risk (29% of SMEs, 32% of large businesses), but are least concerned about health and safety (25% versus 31%). There was no significant variation in risk perception across geographic locations.

Take action: Get help understanding and tackling compliance, legal, and regulatory risks. You can access specialist health and safety training or expert support to assess, improve, and test your health and safety policies and procedures. On top of that, management liability insurance provides cover for a wide range of actions brought against you and your company, spanning data breaches, environmental damage, health and safety claims, and regulatory investigations. Restructuring pensions and other benefits to save on National Insurance costs is an important consideration. Pension regulatory risk is also rising and there are some advantages to using risk insurers to help return to work.

People risks

Which biggest people risks to your business, if any, concern you most?

1. Talent acquisition and retention

28%

2. Employee engagement and morale

28%

3. Mental health and wellbeing

26%

4. Workplace culture and leadership

25%

5. Health and safety of the public and employees

25%

In terms of overall risk, people risks have fallen down businesses' agenda over the last two years, and a similar story plays out here. While the top three specific people risks are unchanged from two years ago — talent acquisition and retention, employee engagement and morale, and mental health and wellbeing — each is cited by marginally fewer businesses.

Talent acquisition risk belies AI hype?

Much has been written and said in recent months about the threat to jobs posed by AI, but talent acquisition and retention remain the top people risk cited by UK businesses. Clearly, we cannot surmise that the threat to jobs is simply not real, though these findings do suggest that any threat that does exist has not yet been felt to any significant degree.

At the same time, businesses' continued focus on engagement, morale, wellbeing, mental health, leadership, and culture may suggest there are no mass replacements for human roles taking place. At the same time, the focus on "softer" people risks may also reflect the HSE's recent decision to place greater emphasis on areas such as mental health and stress in applying existing health and safety regulations.

People risks are still a universal concern

Despite these findings around specific, discrete risks, however, it is important to note that people risks remain a near universal concern. Once again, pointing to the complex web of risks facing UK businesses, 96% of leaders report they do have concerns about at least one people risk.

Sector, size, and geographic variations

Smaller businesses with fewer employees are the least concerned about people risks across the board. Less than a quarter of micro businesses (24%) are concerned about talent acquisition and retention, compared with 30% of large businesses, for instance.

In terms of sectors, those in renewables (67%), communications and media (63%), and technology (40%) are the most concerned about talent acquisition and retention, while agriculture, food and drink, retail, public sector, and recruitment are the least concerned (20–23%). Meanwhile, workplace culture and leadership is a concern for 60% of chemical and life sciences businesses, and not–for–profit organisations are the most worried about employee mental health and wellbeing (45%).

Take action: There is a wide range of help and support available to businesses seeking to manage people risks. For instance, you can review your market position to establish why you could be failing to attract or retain staff. Look at tools to help employee engagement. Make sure what you offer your staff meets their needs and gives you value for money.

Operational and supply chain risks

Which operational and supply chain risks to your business, if any, concern you most?

1. Failure of key suppliers

38%

2. Breakdown of key equipment

35%

3. Failure of key customers

31%

4. Theft of key equipment

25%

5. Logistics

20%

In common with a number of the risk categories covered in this report, business perceptions of discrete operational and supply chain risks have remained broadly unchanged from two years ago, despite slightly more leaders citing this category as a key overall risk (36% today versus 34% in 2024).

For instance, the top two specific risks two years ago — failure of key suppliers and breakdown of key equipment — have each fallen by one percentage point, but remain the leading risks in this area. Failure of key customers and theft of key equipment, meanwhile, show no change from two years ago. On the other hand, logistics risk perception continues to fade, falling again to 20% of businesses, from 27% in 2024.

Steady perception, but it remains a key risk

That is not to say that these risks are being overlooked. The reality is that between two in five, and one in five, businesses cite each of these risks as a key concern, and 93% of businesses say they are concerned about at least one operational and compliance risk.

What's more, the fact that failure of key customers and key suppliers both feature in the top five risks in this area once again points to business perceptions of interconnectivity in the risk environment. Alongside long-standing risks around key equipment, businesses seem abundantly aware of the external risks that flow from increasingly connected, complex supply chains — as is also the case for cyber risk.

Sector, size, and geographic variations

It is no surprise to see those businesses that are more reliant on supply chain partners are the most concerned about the failure of key suppliers, given their increased exposure to these risks. For instance, 80% of chemicals and life sciences businesses worry about this risk, 75% in communications and media, 60% in agriculture, and 44% in construction, contracting, and engineering, say failure of key suppliers is their biggest concern, compared to under a third in education (27%).

Similarly, businesses that rely more on key equipment are the most concerned about breakdowns. Eighty per cent of agriculture businesses, 50% of those in renewables and energy, and 46% in aerospace, defence, and aviation are concerned about equipment breakdown compared with 13% in communications and media and 7% in property and real estate.

In terms of regional variation, the only significant divergence from the mean sees businesses in Northern Ireland more worried about theft of key equipment — 36% cite this risk — than businesses elsewhere (25% on average UK–wide). Broadly speaking, micro businesses, SMEs, and large businesses are aligned in terms of their perception of operational and supply chain risks.

Take action: Businesses can defend against these risks with a combination of insurance and risk management. For instance, you can use machinery damage and breakdown insurance to mitigate the impact if key equipment should break down. Meanwhile, expert help with everything from business continuity planning to rebuild cost assessments and fleet risk is easily available.

Strategic and reputational risks

Which strategic and reputational risks to your business, if any, concern you most?

1. Damage to brand/image

44%

2. New competitor in the market

37%

3. Mergers and acquisitions

29%

4. Governance

27%

5. No strategic and reputational risks

8%

In keeping with Marsh *UK Business Risk Report* findings in 2024, brand damage again emerges as the number one strategic and reputational risk facing UK businesses, cited by 44% of businesses. In fact, of the 47 specific risks businesses were asked about across all risk categories, brand damage is the joint most cited risk, alongside cybercrime (also 44%).

Brand reputation and consequential risk

Brand reputation is arguably the single most interconnected risk facing businesses today. This is a "consequential risk" where damage can flow from incidents in every other risk category — from cyber and compliance to people, operational, and environmental.

It is worth noting here that cyber, while also highly connected, might be described as a "trigger risk." These incidents, as well as causing damage in their own right, can have knock–on effects across other risk areas, including brand reputation.

Waning risk perception masks ongoing concern

Overall, however, and in keeping with a theme emerging in several risk areas, risk perception in this space has decreased slightly. The proportion of UK businesses citing each risk has fallen by one or two percentage points across the board, with the exception of merger and acquisition risk, which has risen slightly from 28% to 29%.

Despite this, it is once again important to note that 92% of businesses remain concerned about at least one strategic or reputational risk.

Sector, size, and geographic variations

Interestingly, power and utilities businesses and those in renewables are among the most concerned about brand damage (80% and 50%, respectively). They are joined by not–for–profit (70%), hospitality, leisure and entertainment (53%), and technology (47%).

The findings also reveal a significant difference in the extent to which businesses in some sectors feel threatened by competition. Half (50%) of respondents in transportation, distribution, and warehousing and automotive, and almost half (49%) of those in technology, say new competition in the market is most concerning, while fewer than three in 10 (26%) of those in the public sector say the same.

Similarly, merger and acquisition risk is felt most acutely by businesses in Wales (39% versus 29% on average), while those in Northern Ireland are most worried about new competitors (41%). At the same time, micro businesses are more worried about brand damage (45%) and new competition (40%) than their larger counterparts — SMEs report 44% concern for brand damage and 38% for competition, compared to 42% and 34% for large businesses, respectively.

Take action: In this age of interconnected risk, there is a great deal businesses can do to manage strategic and reputational risk at the root cause. That could involve reviewing employers' liability and professional indemnity insurance to ensure adequate cover is in place. Equally, it could mean looking into insurance cover such as directors' and officers' liability and management liability — both of which can help minimise reputational damage if the worst should happen. Don't forget that people are brand ambassadors and can cause significant reputation risk. Having a happy, engaged workforce and external relationships is key to limited reputational or brand damage.

Environmental risks

Which environmental risks to your business, if any, concern you most?

1. Extreme temperatures and weather events

31%

2. Environmental damage/pollution

27%

3. Natural disasters

23%

4. Net zero

19%

5. Greenwashing

18%

As we have seen, environmental risk as a whole remains outside the top five risk categories, and at first glance, businesses appear less concerned about environmental issues across the board. In fact, extreme temperatures and weather events are the only risks that seem more concerning to businesses in 2026 (31% in 2026 compared with 30% in 2024).

Declining risk perception?

It is a concern to see business leaders apparently far less troubled about issues such as environmental damage and pollution (down to 27% from 33%), especially given that the cost of pollution events, with the Environment Agency levying fines totalling £3.8 million in 2024.

Equally, just 19% of business leaders see net zero as a risk, compared with 26% in 2024, while concern over natural disasters has declined by five percentage points over the same period.

We can only speculate as to what has driven this decline in concern over environmental risks. It is possible that the government's move to water down green initiatives, as well as wider political rhetoric on the subject, has played a part.

Extreme weather is a major concern

All that said, the scale of the concern around extreme weather should not be underestimated — 31% of UK businesses equates to almost 1.8 million businesses with real worries around issues such as extreme temperatures and weather events. Similarly, just under a million businesses (16% — 912,000) say they are concerned about flooding. In fact, overall, 83% of UK businesses say they are concerned about at least one environmental risk.

Sector, size, and geographic variations

Once again, variations in risk perception in this area fall in line with broadly predictable sector considerations.

For instance, concern about extreme weather is highest among sectors for which weather and climate have a material effect on performance. Agricultural businesses (80%) are the most aware of these risks, followed by renewables (50%), and power and utilities (40%). It is perhaps surprising to see only 37% of retail businesses concerned about extreme weather, given the effect prevailing conditions can have on footfall, but less surprising to see communications and media entirely unconcerned (0%).

Given the concern over watercourse pollution, it is again a surprise to see only 20% of power and utilities and 20% of agricultural businesses worrying about environmental damage and pollution, far behind renewables at 67%.

In terms of net zero, agricultural and chemical/life sciences businesses (both 0%) are the least concerned, while communications and media (50%) and power/utilities (40%) are the most concerned.

Meanwhile, Scottish businesses are more concerned than average about net zero (27% versus 19%), and Northern Irish businesses are the most worried about extreme weather (35%).

Take action: Businesses may be more worried about environmental risk than they were 12 months ago, but that concern remains relatively low, despite the real impacts that can flow from environmental incidents.

The good news is that there is plenty of support available for those keen to act. For instance, environmental liability, pollution liability, and management liability insurances can help to mitigate impacts in the event of an incident, while flood insurance can help your firm to recover if its premises are affected by flooding.

Social and geopolitical risks

Which social/geopolitical risks to your business, if any, concern you most?

1. Future pandemic

33%

2. Political unrest

28%

3. War/conflict

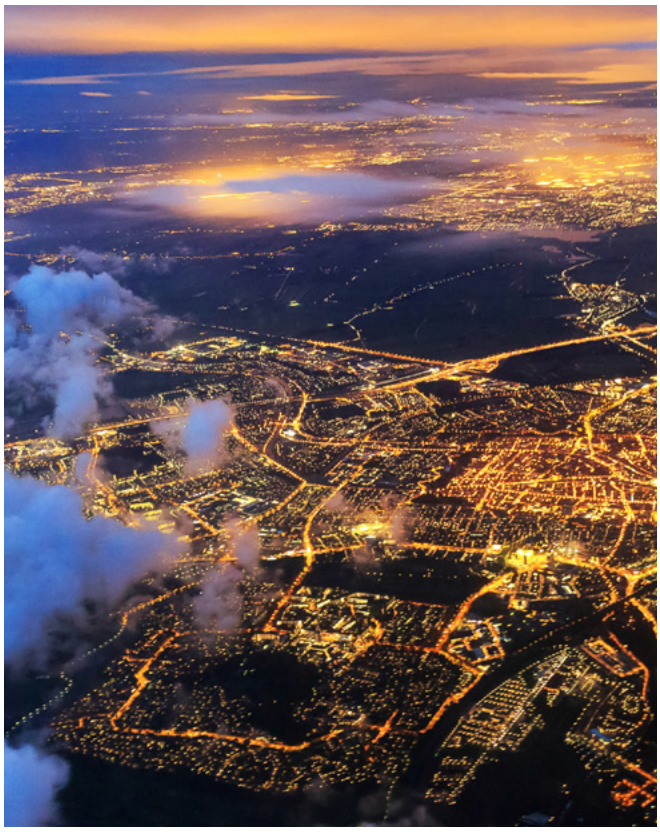
23%

4. Climate risk

22%

5. Terrorism

18%



It is clear that the disruption unleashed by the COVID–19 pandemic remains fresh in the memories of many businesses, with future pandemics ranking as the top social and geopolitical risk for 33% of UK businesses.

Pandemics ahead of politics, war, and climate

As in 2024, direct risk experience still trumps very real and present risk. Pandemic risk is still well ahead of political unrest (28%), despite real political turbulence at home and abroad, and ahead of war and conflict (23%). At the same time, battle continues to rage in Ukraine, on the doorstep of Europe. Additionally, the Middle East crisis has developed since conducting the survey.

In keeping with the faltering perception of environmental risk we have already seen, climate risk is down one place to fourth, cited by 22% of businesses compared with 26% in 2024. Terrorism ranks among the top social and geopolitical risks for business leaders, cited by 18% of responses, down from 19% two years ago.

Again, despite the apparent weakening of concern across the top risks in this area, it is worth remembering that 88% of businesses still say they are worried about at least one social and geopolitical risk.

Sector, size, and geographic variations

The sectors most directly affected by the COVID–19 pandemic are also the ones most concerned about future pandemic risk. Almost half (45%) of not–for–profits, 41% of health and care, pharmaceuticals, and health and beauty, and 39% of education organisations cite pandemic as a key risk.

When it comes to war and conflict, agriculture (40%) and chemicals/life sciences (40%) businesses are the most concerned, while communications and media (13%) and the public sector (14%) are the least concerned.

Meanwhile, power and utilities businesses are the most concerned about terrorism, climate risk, and activism (all 40%). Finally, larger businesses are more worried about political unrest than their smaller counterparts — 30% of large businesses cite this as a risk compared with 26% of micro businesses.

Take action: It is crucial to prepare for the unexpected. A business continuity plan helps prepare you for the worst and limit the potential impact to your business operations, ensuring you can continue to work and earn. Employee engagement and a flexible working strategy can help support hybrid working, if required, during periods of unrest. Ensure that your cybersecurity policies and procedures covers potential instances when your workforce may be working remotely.

Putting in context a diverse web of risk

At this stage, it is worth pausing to put the sheer range of risks businesses perceive as threats into context.

Across the seven risk categories set out on the previous pages, businesses rated a total of 47 risks in terms of the level of threat they represented — 47 risks that are themselves a mere cross-section of the actual total risk environment. Of those 47 risks, 36 were selected by at least 20% of businesses, and none were considered to pose no threat.

While that scale alone is daunting, setting those risks out in order of perceived threat level, rather than by category, gives a flavour of the complexity businesses are dealing with.

Then factor in that the weight given to each risk, and therefore their order of importance, varies widely from sector to sector — and that many of these risks are interconnected — and the picture of a complex web of risk starts to emerge.

Top 40 responses drawn from seven major risk categories

Rank	Risk	Businesses concerned
1.	Cybercrime	44%
2.	Damage to your brand/image	44%
3.	Failure of key suppliers	38%
4.	New competitor in the market	37%
5.	Breakdown of key equipment	35%
6.	Service disruptions	33%
7.	Future pandemic	33%
8.	Introduction of new rules or legislation	32%
9.	Extreme temperatures and weather events	31%
10.	Failure of key customers	31%
11.	Changes to tax/National Insurance	30%
12.	Economic instability	30%
13.	Digital transformation (for example, AI, ChatGPT)	29%
14.	Health and safety	29%
15.	Mergers and acquisitions	29%
16.	Political unrest	28%
17.	Internal IT network disruption	28%
18.	Talent acquisition and retention	28%
19.	Employee engagement and morale	28%
20.	Environmental damage/pollution	27%
21.	Governance	27%
22.	Insider threat	26%
23.	Mental health and wellbeing	26%
24.	Workplace culture and leadership	25%
25.	Health and safety	25%
26.	Risk of recession	25%
27.	Theft of key equipment	25%
28.	Employment law	24%
29.	Natural disasters	23%
30.	War/conflict	23%
31.	Fraud/corruption	23%
32.	Climate risk	22%
33.	Inflation	22%
34.	Trade tariffs/relationships	21%
35.	Cash flow	20%
36.	Logistics	20%
37.	Net zero	19%
38.	Cost of insurance	19%
39.	Administration and technology	19%
40.	Terrorism	18%

The steps businesses have taken to manage key risks

Driving resilience

Have you reviewed the following in the past year?

1. Employee training

53%

2. Health and safety management

49%

3. Staff levels review

49%

4. HR and employment law

47%

5. Pay review/cybersecurity controls

46%

At first glance, it appears that businesses are taking less action to build resilience as well as manage and mitigate risk across the board. Two years ago, the top actions were taken by between 62% and 57% of businesses, while in 2026, those figures have dropped to 53% and 46%.

In some cases, this seems to be true. For example, 58% said they had reviewed business contingency plans in 2024, compared with 45% this year. Similarly, in 2024, 55% said they had reviewed their insurance arrangements, a figure that dropped to 45% in 2026. We should, however, view that reduced focus on reviewing insurance in the context of business leaders who are less worried about the cost of insurance than they were two years ago (21% in 2024, versus 19% in 2026).

Focus on trigger risks?

On the other hand, a closer look at the findings suggests businesses are taking a targeted approach to managing and mitigating risk, building on the significant investments they made during 2024. Indeed, it appears they may be focusing on the "trigger" risks that can have wide-ranging impacts, fanning out across multiple risk areas.

For instance, as we have seen, cyber risk can have serious implications in almost every other risk area — a fact businesses seem well aware of, given its position at the top of leaders' key risks. In turn, reviewing cybersecurity controls is now, for the first time, among the top five actions businesses take to manage risk and build resilience.

Continued focus on people risks

People risks, though only fourth on businesses' list of key risks, is clearly a trigger risk — adverse incidents here can fan out across compliance, finance, brand, and reputation, while the actions of employees can also precipitate cyber risk and environmental risk.

Small wonder then, that we continue to see a real focus on this area, with all five of the top actions attributable to managing people risk. Employee training takes top spot, reviewed and updated by 53% of businesses, with health and safety management (49%), staff levels reviews (49%), HR and employment law (47%), and pay reviews (46%) not far behind.

In fact, of the 10 people risk management reviews businesses were asked about, all were carried out by at least 42% of businesses, which further serves to demonstrate the concerted, multi–faceted action being taken in this area:

- Employee training (personal and professional development) — 53%
- Health and safety management (people and process) — 49%
- Staff levels review — 49%
- HR and employment law (people policy and process) — 47%
- Cybersecurity controls (including use of AI) — 46%
- Pay review (benchmarking) — 46%
- Employee health and benefits offering — 45%
- Mental health support — 44%
- Workplace culture and leadership — 44%
- Workplace pensions — 42%

Concerted, diverse action

In truth, the range of 16 actions businesses were asked about represents only a small cross-section of the risk management and resilience landscape.

However, business leaders' responses give a sense of concerted, wide-ranging action. In short, UK businesses are continuing to make real investments in building resilience, even when faced with such a daunting, diverse web of risk:

Have you reviewed the following in the past year?

Rank	Risk management action	proportion taking action
1.	Employee training (personal and professional development)	53%
2.	Health and safety management (people and process)	49%
3.	Staff levels review	49%
4.	HR and employment law (people policy and process)	47%
5.	Cybersecurity controls (including use of AI)	46%
6.	Pay review (benchmarking)	46%
7.	Employee health and benefits offering	45%
8.	Insurance coverage	45%
9.	Business contingency plans	45%
10.	Supplier and/or customer review	45%
11.	Mental health support	44%
12.	Workplace culture and leadership	44%
13.	Adoption of new technology to support your operations	44%
14.	Workplace pensions	42%
15.	Risk registers	41%
16.	Environmental, social, and governance framework (ESG)	36%

Targeted resilience breeds confidence

Interestingly, this targeted action to build resilience appears to have left the majority of business leaders feeling confident in their ability to navigate real challenges. Almost two–thirds (62%) said they felt confident that their business's risk management framework would enable them to successfully navigate risks associated with government budgets, such as fiscal sustainability, inflationary pressures, and political risks.

Sector, size, and geographic variations

In general, businesses in the south of England and London are more likely to have reviewed their risk management capabilities than those elsewhere in the country.

For instance, businesses in London are the most likely to have reviewed their cybersecurity controls (58%), while those in Northern Ireland are the least likely (28%). Similarly, those in the south of England (63%) and London (60%) are more likely to have reviewed employee training than those elsewhere in the UK, with Northern Irish businesses again the least likely to have done so.

In a similar vein, the larger the company, the more likely it is to have taken action to manage risk. For example, 53% of large businesses have reviewed their cybersecurity controls, compared with 34% of micro businesses and 48% of SMEs. Equally, 59% of large businesses have reviewed employee training, compared with 40% of micro businesses and 56% of SMEs.

Perhaps not surprisingly, given the variations outlined above, business leaders in the south of England (70%) are among the most likely to say they feel confident in their risk management frameworks, while those in Northern Ireland (55%) are among the least likely.

How businesses are investing to thrive in the face of ever-changing risk

Scanning the horizon

What, if anything, do you plan to invest in most to manage your key risks over the next 12 months?

1. Employee training (personal and professional development)

23%

2. Cybersecurity controls (including use of AI)

22%

3. Adoption of new technology to support their operations

21%

4. Employee health and benefits

19%

5. Mental health support

19%

6. Health and safety management

18%

7. Pay review

17%

Over the next 12 months, it seems the main focus of businesses' risk management efforts is to build on the investments they have already made.

On the face of things, the numbers above seem low, but they must be viewed in context. For instance, as we have seen over several Marsh *Business Risk Reports*, businesses have tended to understate their investment plans, compared with the actions they take in reality, as reported in hindsight the following year.

Building on previous investment

The breakdown above again suggests a focus on progressive improvement, with plans appearing very much in line with the investments businesses have already made. For instance, where 53% of businesses invested in employee training during 2025, 23% report firm plans to do so in 2026. It's a similar story across the board:

- 22% plan to invest in cybersecurity controls, where 46% have already done so.
- 18% plan continued investment in health and safety management (49% in 2024).
- 17% plan to carry out pay reviews, where 46% did so in 2024.

Alongside that, we can see a broadening of focus in investments to manage people risk. For example, plans to strengthen employee health and benefits and mental health support both feature in the top five investments for 2026, having previously fallen outside the top five investments already made.

Investments must be consistent

The caveat is that, if we take the relatively low numbers above at face value, this would be cause for concern. In the end, risk management must be a continuous and consistent focus if businesses are to avoid letting the benefits of previous investments erode by allowing vulnerabilities to build.

That said, it should also be noted that just 4% of businesses said they had no plans to invest in managing key risks over the next 12 months.

Sector, size, and geographic variations

As expected, there are significant variations in investment plans across sectors. For example, critical infrastructure providers such as those in power and utilities (60%) and technology (54%) are far more likely to invest in cybersecurity than the average (22%), as are not–for–profits (50%) and those in chemicals and life sciences (40%).

Meanwhile, perhaps surprisingly, not–for–profits are among the most likely to invest in risk management across the board. Half say they plan to invest in cybersecurity, 45% in employee training, 35% in new technology to support operations, 30% in employee health and benefits, and 30% in mental health support — all well above average.

The picture is more mixed regionally, with businesses in London most likely to invest in employee training (26%), cybersecurity (26%), and new technology (27%), but among the least likely to invest in people-related risk management. Here, Scottish businesses are the most proactive, with 24% focusing on employee health and benefits and 25% planning to strengthen mental health support.

When it comes to business size, perhaps surprisingly, SMEs are the most likely to invest in employee training (25%) and health and safety management (19%), outstripping even their larger counterparts (22% and 17% respectively).

Micro businesses are the least likely to invest in all areas except mental health support, where 18% plan to strengthen their mental health support, compared with 17% of SMEs. This reticence to invest is particularly true when it comes to cybersecurity, a focus for 13% of micro businesses, compared with 24% of both SMEs and larger businesses.

Take action: Help is available for firms committed to realising the benefits that can flow from improved training and controls. For instance, you can start by reviewing your cybersecurity policies and procedures. Read these 12 key controls to help strengthen your cybersecurity. Equally, you can access specialist health and safety training or expert support assessing, improving, and testing your health and safety policies and procedures.

Digitalisation is reshaping businesses including employee benefits offerings, enabling employers to give their people more personalised, accessible, and innovative offerings.

The tools and technology to adapt

How businesses are evolving to streamline risk and insurance

Do you currently use or would you like to use in the future any of the following digital tools or technologies to identify, manage, or mitigate insurance–related risks?

Current use

1. Learning/training platform

48%

2. Cybersecurity solutions

46%

3. Data analytics

45%

4. Online client portal (access to policy documents)

42%

5. Risk management software

37%

6. IoT devices (a network of connected devices that exchange data via the internet)

33%

7. Online renewal systems

30%

Current use and would like to use

79%

1. Learning/training platform

78%

2. Cybersecurity solutions

78%

3. Data analytics

77%

4. Online client portal (access to policy documents)

76%

5. Risk management software

72%

7. Online renewal systems

71%

6. IoT devices (a network of connected devices that exchange data via the internet)

Another reason to view risk management investments through a positive lens, and a sign that UK businesses are reacting with purpose to the sheer complexity of the risk environment, comes in their current and planned use of digital tools and technologies to streamline efforts to identify, manage, or mitigate risks.

That is, while between half (48%) and a third (30%) are already using these tools, between 79% and 71% would like to use them in future.

Currently, the tools most commonly in use are learning and training platforms (48%), cybersecurity solutions (46%), data analytics (45%), and risk management software (37%). Meanwhile, 42% use online portals to access insurance documentation and tools and 30% use online insurance renewal systems.

However, those numbers appear modest when compared with the level to which businesses want to use these tools. Close to eight in 10 (79%) either use or would like to use online and training platforms, while a large majority say the same about cybersecurity solutions (78%), data analytics (78%), risk management software (76%), and connected, Internet of Things (IoT) devices (71%).

Similarly, a clear majority also wants to streamline insurance administration. More than three quarters (77%) want to use online portals to access insurance documents and tools, and 72% either use or would like to use online insurance renewal systems.

Flexible resilience?

Taken in combination with continued efforts to manage risk, we can see these near-universal plans to invest in streamlining risk management and insurance as very much part of businesses' desire to evolve and adapt in the face of complex risk.

Across both risk management and these technologies, the focus on people, skills, wellbeing, data, connectivity, and cyber risk can be read as

attempts to gather and strengthen the skills and tools required to build a measure of adaptability and flexibility into business resilience.

This flexibility and agility is, it can be argued, very much what businesses need to adapt in a complex risk environment where interconnected perils can interact to create new risks quickly.

Sector, size, and geographic variations

Generally speaking, larger businesses with deeper pockets and more complex risk exposures are more likely to be using or want to use these tools.

For instance, 84% of large businesses want to use cybersecurity controls, compared with 66% of micro businesses and 79% of SMEs, while 89% of large businesses either use or want to use risk management software, compared with 66% of micro businesses. Similarly, 83% of large businesses say the same about online learning platforms, compared with 71% of micro businesses. Micro businesses are also least likely to use or want to use data analytics (72%), versus 83% of large businesses and 77% of SMEs.

It is a similar story when it comes to tools to streamline insurance administration, with larger businesses more likely to use them. However, it is worth noting that, at the moment, only around a third to a quarter actually do so.

In terms of variations between sectors, we see this mainly in the split between businesses currently using tools and those for whom their use is an ambition. For instance, 75% of communications and media companies presently use cybersecurity solutions, and 13% plan to use them in the future. On the other hand, 41% of construction, contracting, and engineering businesses currently use these tools, while 36% want to use them in future.

As with efforts to review risk management over the last 12 months, businesses in the south of England and London are generally more likely to either use or want to use these tools than businesses elsewhere in the country.

Take action: Consider harnessing innovative technologies, such as risk analytics, telematics, online renewals and insurance portals. This can empower your business with solutions that enhance your risk management, streamline operations and deliver meaningful risk insights. Which in turn helps you confidently navigate the complexities of risk and insurance.

About the research

The fifth edition of the Marsh UK Business Risk Report draws on the views and experiences of 2,169 respondents across the UK.

The survey was completed by 169 business leaders drawn from Marsh clients and clients of Marsh's family of businesses (Marsh, Marsh Commercial, Mercer Marsh Benefits, SMEi, Bishop Skinner Marine, and Hamilton Bond), as well as 2,000 leaders from the wider population of UK businesses.

Respondents were questioned between 30 December 2025 and 23 January 2026, and were qualified according to company size, seniority, age, location, industry, business type, and Marsh client status.

For this report, our business sample has been segmented as follows:

- Micro businesses: 0-20 employees.
- SME: 21–250 employees.
- Large businesses: More than 250 employees.

About Marsh

We are the world's leading professional services firm in risk, strategy and people. We bring together experts across Marsh, Guy Carpenter, Mercer and Oliver Wyman to help our clients see what's possible, mobilise their people and manage risk as they navigate new pathways. For more information, visit marsh.com, or follow us on LinkedIn.

25101520-UK