



Adaptation and resilience in the United Kingdom



Executive summary

Geopolitical tensions, cyber threats, energy insecurity, supply chain disruption and declining public trust are increasingly converging in the UK, alongside the long-term impact of the changing climate, creating a more complex and interconnected risk landscape.

Cyber threats have become one of the most immediate challenges to business continuity and economic performance. Yet many organisations remain underprepared, lacking clear board-level accountability, robust response plans and effective oversight of supply chain vulnerabilities. Other strategically significant risks include economic fragility, workforce constraints, AI-related liabilities, extreme weather events, energy security concerns and geopolitical disruption.

A notable disconnect has also emerged between executive priorities and public concerns. While business leaders focus on cyber security, technology and operational resilience, public attention is increasingly centred on the cost of living, misinformation and trust in institutions. This gap presents a communication challenge: organisations must not only manage risk effectively but also explain their resilience efforts in ways that stakeholders understand and trust.

It is essential to understand that changes to the environment remain a key driver of corporate and public concern and geopolitical instability, even if there is a sense they are being superseded by more immediate concerns. Their relevance has been downgraded by political opposition to environmental initiatives, particularly from the US administration, which has prompted

a short-term retreat from governmental and corporate commitments. However, a summer marked by record temperatures and droughts, particularly across Europe, has provided a renewed focus on the need to manage the fallout from climate change.

However, the emphasis is shifting from mitigation towards resilience and adaptation to the effects of a warming world. At the same time, resilience is moving from best practice to regulatory expectation, with increasing legal, reporting and preparedness obligations for businesses. This change is also reflected in corporate reporting with an increasing need to show tangible corporate outcomes while reducing the emphasis on disclosure for its own sake.

Forward-looking organisations ensure that resilience represents more than a compliance requirement. Managed effectively, it can become a source of competitive advantage and strategic trust.

Organisations should aim to understand their exposure, prioritise their risks and strengthen their response through a combination of risk analysis, stakeholder mapping, foresight, narrative development and implementation planning. The result should be a clear and actionable resilience roadmap that enhances operational preparedness while building long-term trust.

1. The UK resilience landscape

Resilience has become a defining challenge. Although traditionally associated with the ability of communities and ecosystems to recover from shocks, it is now understood more broadly as the capacity of societies, economies and governments, as well as individual companies, to anticipate, adapt to and recover from disruption while continuing to function effectively.

Resilience covers a wide range of interconnected long- and short-term issues, including climate change, nature conservation, food security, economic stability, political governance, and digital and cyber security. Physical security is also becoming an increasingly important part of the discussion.

Climate change is bringing more frequent extreme weather events, including this summer's high temperatures and low rainfall. Geopolitical tensions are affecting energy and food supplies. Digital technologies create vulnerabilities alongside new opportunities. Political developments, meanwhile, continue to reshape governance and economic priorities at a rapid pace.



POLITICAL INSTABILITY

The UK has faced a particular combination of pressures in recent years. The effects of the 2007-08 global financial crisis were especially severe because of the country's heavy reliance on the financial services sector. These pressures were later compounded by Brexit, the COVID-19 pandemic, and disruptions to global energy markets linked to the conflicts in Ukraine and, more recently, the Middle East.

The UK political environment has moved to a fragmented landscape. The two main parties still command the largest share of votes and parliamentary seats, but political loyalties have become less predictable and more fluid. This has given smaller parties greater opportunities to exert influence. Populist parties and politicians increasingly frame politics as a contest between ordinary citizens and a distant establishment elite, drawing on concerns around economic inequality, immigration, public services and trust in institutions. The political environment is therefore more diverse, contested and unpredictable than it was a decade ago.

A resilient organisation needs to be able to absorb these shocks while maintaining employment, supporting businesses and protecting living standards. However, that requires a plan that includes sustained investment in skills, innovation and infrastructure.



DIGITAL AND CYBER RESILIENCE

The UK National Cyber Security Centre has identified cyber resilience as a critical priority, warning that cyberattacks represent a growing threat. Digitalisation has improved efficiency enormously but it has also created new vulnerabilities.

In 2025 alone, big names including Marks & Spencer and Jaguar Land Rover suffered major attacks, and the 2024 ransomware attack on Synnovis, an NHS supplier, caused widespread disruption to blood testing and thousands of medical appointments. The short-term impact on economic activity is damaging – the Jaguar Land Rover attack contributed to a measurable GDP contraction – but the threat to long term confidence is perhaps worse.



ENERGY RESILIENCE

A reliable and resilient energy supply is becoming more important to economic stability as electricity demand increases. Much of the UK's electricity infrastructure was built during the 1950s and 1960s and is approaching the end of its intended operational life. We now urgently need a shift from a largely reactive approach towards a more proactive and predictive model.



CLIMATE CHANGE, ADAPTATION AND NATURE CONSERVATION

All these issues are compounded by the long-term impacts of climate change. As the physical effects of a warming climate become more pronounced, adapting to changing conditions has moved to the centre of the UK political agenda, complementing efforts to curb emissions.

The shift towards a lower-carbon economy offers a potential dividend: greater energy independence and reduced exposure to volatile fossil fuel markets. Economic strength and environmental stewardship are becoming increasingly intertwined, making it harder for UK policymakers and business leaders to treat them as separate challenges.

While recent political resistance to environmental initiatives has tempered enthusiasm for ESG in some quarters, recent extremes in temperature and water scarcity across Europe have reinforced the economic and societal costs of inaction. As a result, UK Government attention is increasingly turning from prevention alone to preparedness and resilience.

This recalibration is also reshaping priorities of the business community. Companies are being judged more on the effectiveness of the measures they implement, and boards face growing pressure to demonstrate tangible progress and embed long-term resilience thinking into strategic decision-making.

At the same time, organisational preparedness is shifting from a matter of good governance to a regulatory requirement. The UK government is building capacity around planning and operational readiness, reflecting a broader recognition that resilience is no longer optional.



FOOD SECURITY AND SUPPLY CHAIN RESILIENCE

The UK has traditionally relied heavily on international trade to supplement domestic food production. While this provides access to a diverse range of products, it also creates exposure to disruptions caused by geopolitical tensions, extreme weather events, disease outbreaks and global market volatility. Covid disrupted transport and labour availability, while the conflicts in Ukraine and the Middle East have affected grain and fertiliser markets.

Climate change is placing additional pressure on agricultural systems: according to the Agriculture and Horticulture Development Board, the UK's 2026 cereal yields were around 15% lower than the ten year average because of the hot, dry weather. Strengthening food resilience will require greater support for sustainable domestic agriculture, investment in climate-resilient farming techniques, stronger local supply chains, and technological innovations such as precision agriculture and advanced crop management systems.

Digital resilience starts with defending against cyber threats. It also means maintaining reliable communications networks, protecting data and ensuring continuity during system failures.

The sections that follow examine where UK assessments, executive concern, measured company experience and public sentiment align on the risks that matter most today, and where they differ.

2. Growing risks

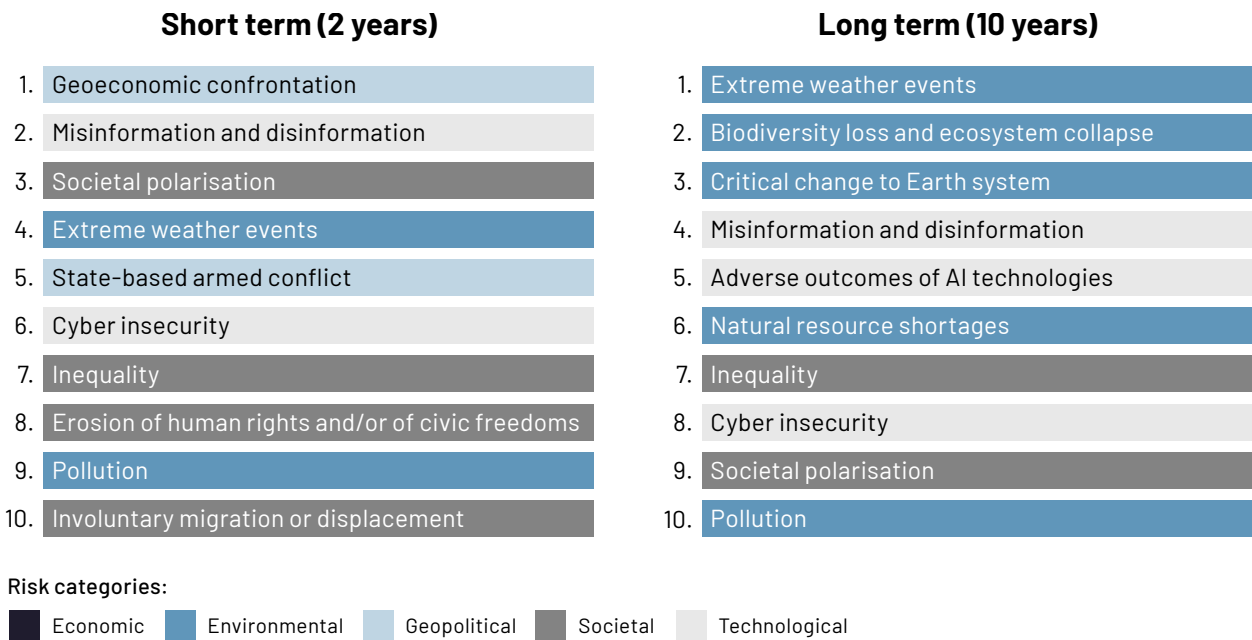
The WEF 2026 benchmark

The World Economic Forum runs a Global Risks survey each year, and for the first time, geoeconomic confrontation tops short-term ranking, ahead of misinformation and disinformation, societal polarisation, extreme weather events, and state-based armed conflict. Economic risks post the sharpest rises in the survey. Climate change, in different iterations, played a prominent role in the list of long-term risks.

The ranking is a reference frame not a forecast, and its value to corporate leaders lies in stress-testing which of the categories are already active in a company’s own markets and supply chains, and therefore have an impact on its licence to operate.

Since the UK economy is such an important part of global finance, data flows and trade, very little can be ruled out on geography alone.

Global risks ranked by severity, short term and long term



Nearly a third of respondents cited either geoeconomic confrontation or state-based armed conflict as the risk most likely to trigger a material global crisis in 2026. Trade, finance and technology have become instruments of state competition, and the disruption they generate arrives through commercial channels, in tariffs, sanctions, export controls, price shocks and degraded information environments, long before it registers as a security event.

Building a UK executive risk map

Despite the breadth of issues impacting the UK, it is important to refine the list to business-critical factors UK organisations can address by examining:

1.

What the state assesses

2.

What executives say they fear

3.

What official statistics show companies *actually* experience and do

4.

What the public feels

Each of these four signals captures a different dimension of the risk environment. Read together, they allow companies to distinguish background noise from material developments and to identify where attention is most urgently required.



State assessments and resilience obligations

The British Government publishes an unusually detailed account of its own vulnerabilities. The National Risk Register 2026, published by the Cabinet Office in July, catalogues around 95 acute risks, rating a pandemic and a cyberattack on infrastructure among the most severe. The Chronic Risks Analysis, from 2025, tracked a further 26 slow-burn pressures that wear down workforce, fiscal and institutional capacity.

The Government has also built the machinery, creating one crisis-management structure with billion pound budgets, resilience training for thousands of people and a Cyber Resilience Index for critical national infrastructure.

The most consequential shift for companies is legal, with both legislation and statutory guidance moving resilience from something government recommends to something it requires. Part of the national preparedness burden is being formally transferred to business.

THE MAIN SHORT-TERM RISK THEMES ARE:

- Cyber and digital vulnerability across infrastructure, data and supply chains
- Pandemic and biosecurity exposure as a persistent top-tier state concern
- Sabotage, state threats and interference targeting infrastructure and democratic processes
- Chronic risks that erode workforce, fiscal and institutional capacity over time
- Environmental concerns around extreme weather, biodiversity loss and natural resource shortages
- Resilience obligations migrating from guidance into law

Executive concerns

In several different surveys, including the WEF Executive Opinion Survey, the Marsh UK Business Risk Report and the Allianz Risk Barometer, UK business leaders have focused on the downstream impact of geopolitics, where it impacts on growth, public services, labour and the information environments. Concerns about digital risk are firmly established high on the executive agenda.



Exposure and preparedness

While the Cyber Security Breaches Survey 2025/26 found that 43% of businesses identified a breach or attack in the previous twelve months, only 31% of businesses assign board-level responsibility for cyber security. And only 25% hold a formal incident response plan, and 15% review the cyber risk in their immediate supply chain.

Yet, as was the case with Jaguar Land Rover, a single failure can now escalate into a national economic event.

Public and stakeholder sentiment

The wider public are not clamouring for action on these major issues. The Ipsos Issues Index shows immigration is the leading public concern, ahead of the economy, the NHS and inflation. Interest in defense spending fluctuates depending on the perceived threat but is still relatively low down the list.

Cyber risk, which dominates both the state’s assessments and the executive agenda, appears nowhere in these public rankings.

The overall sense is one of skepticism: the GfK Consumer Confidence Barometer has not returned a positive reading in a decade. And the NatCen’s British Social Attitudes series shows very low trust in the Government putting the country before party.



3. Media themes

The four signals above describe what institutions assess, what executives report and what the public tells pollsters. We also tracked six short-term thematic clusters across UK editorial media, social platforms, blogs, forums and comments to assess what the country is actually talking about, how much attention each issue receives, or in what tone:

1.

Cyber and digital operational resilience
2.

AI as a business risk
3.

Economic, workforce and skills pressures
4.

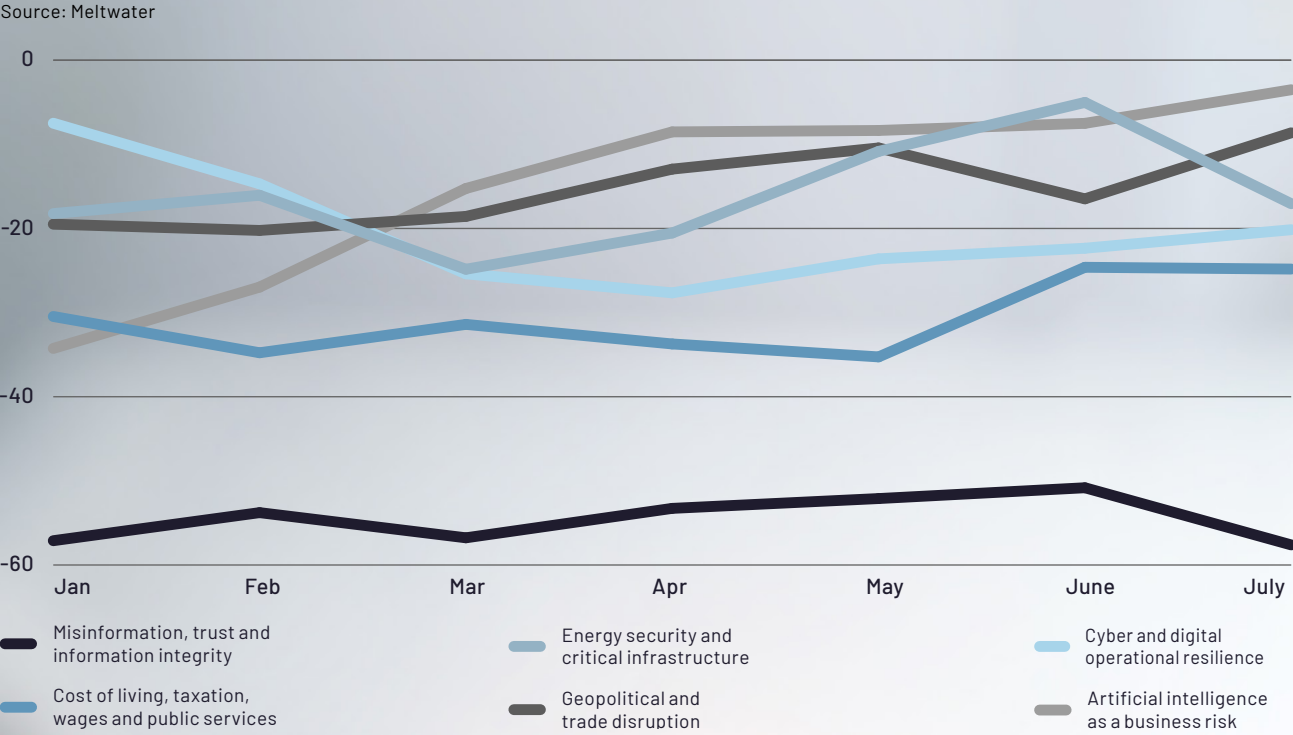
Geopolitical, trade and regulatory disruption
5.

Supply chains and critical infrastructure
6.

Reputation, misinformation and stakeholder trust

Our parameters were 1 January and 29 July 2026, and we used Meltwater. The exercise returned 2.88 million mentions.

Average sentiment trend in United Kingdom
Jan 2026 - July 2026



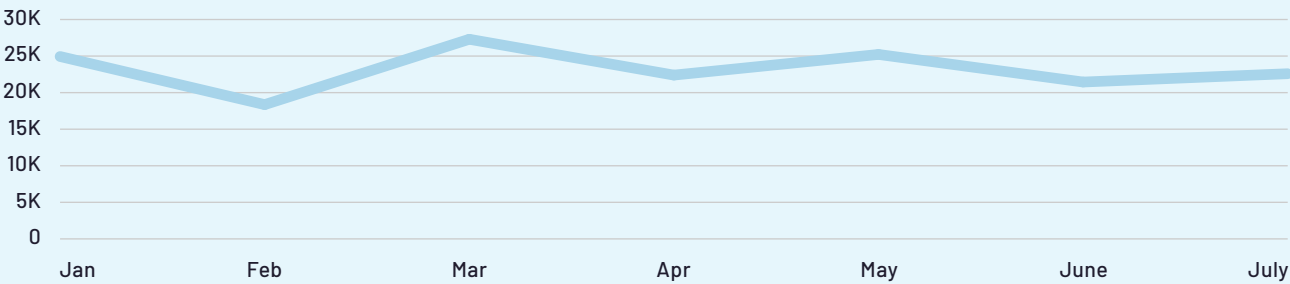
The distribution of that volume across the six themes is itself revealing.

What is very striking is that this ranking is almost the inverse of the executive one, with cyber being the second smallest cluster in national conversation.

What each cluster actually measures

The keyword profiles show that the labels attached to the clusters do not always perfectly reflect what the searches returned.

Total mentions - Cyber and digital operational resilience
Jan 2026 - July 2026

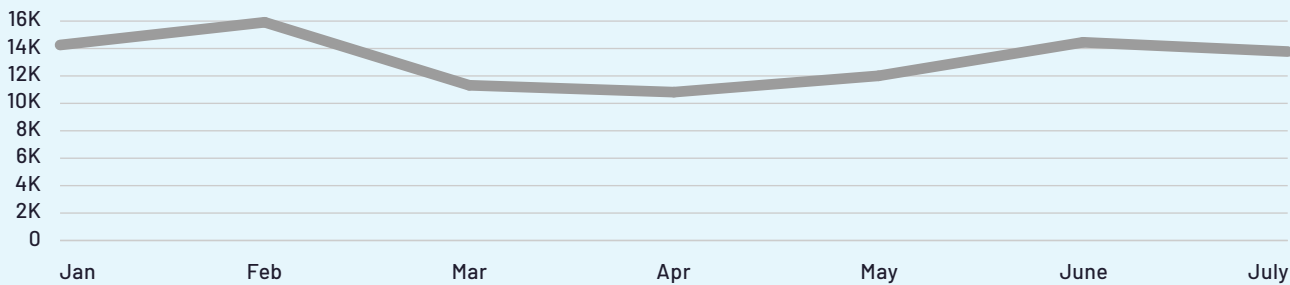


Source: Meltwater



The **cyber cluster** returned the expected core terms, including data breach, cyber attack, personal data, sensitive data, customers and security.

Total mentions - Artificial Intelligence as a business risk
Jan 2026 - July 2026

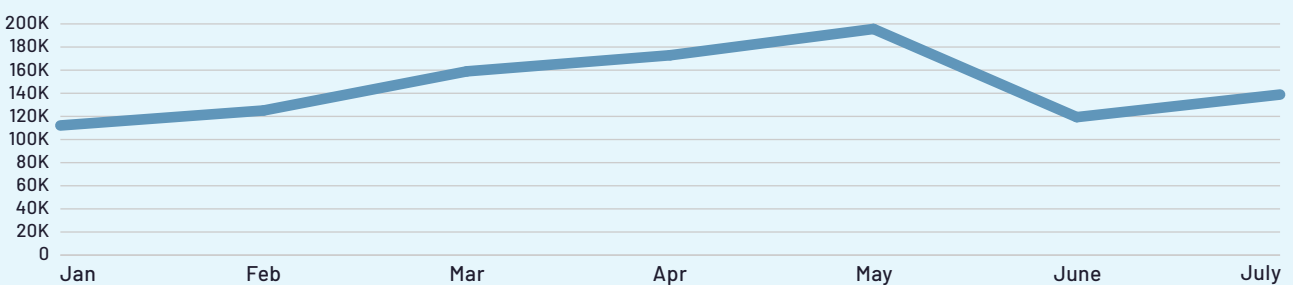


Source: Meltwater

The **AI cluster** is dominated by AI governance, AI safety, AI systems, technology and jobs, which corresponds to the intended subject. Children and fake account also appear prominently, reflecting the UK's online safety debate rather than AI specifically as a business risk.

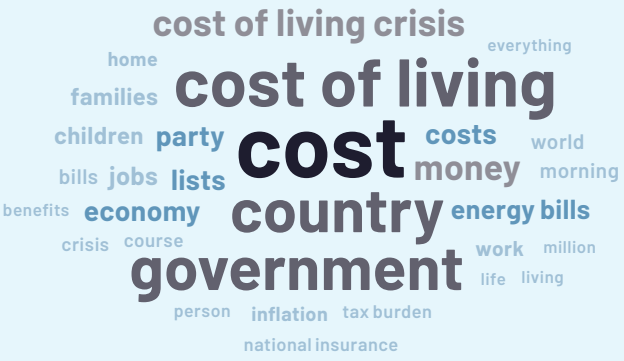


Total mentions - Cost of living, taxation, wages and public services
Jan 2026 - July 2026

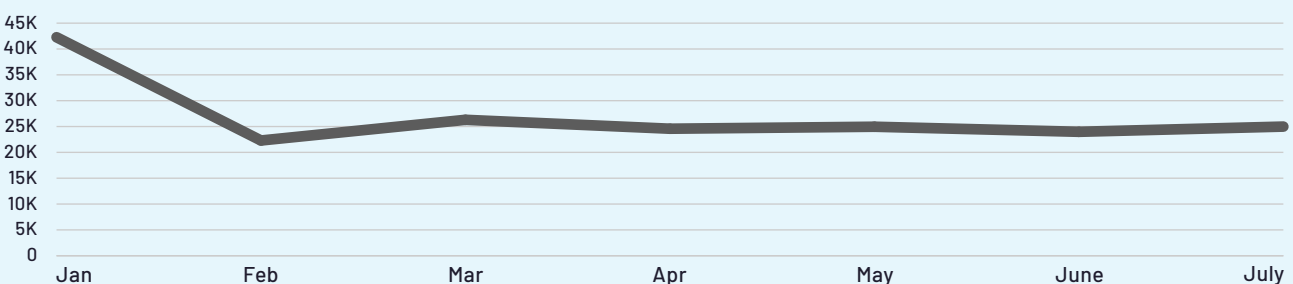


Source: Meltwater

The **economic cluster** was overwhelmingly centred on households. The cost of living crisis, energy bills, families, benefits, money and inflation dominated the profile. The tax burden, including National Insurance, are the main terms that relate directly to employers. The 1.02 million mentions therefore describe public financial pressure more than corporate workforce risk, an important distinction when interpreting the overall volume.

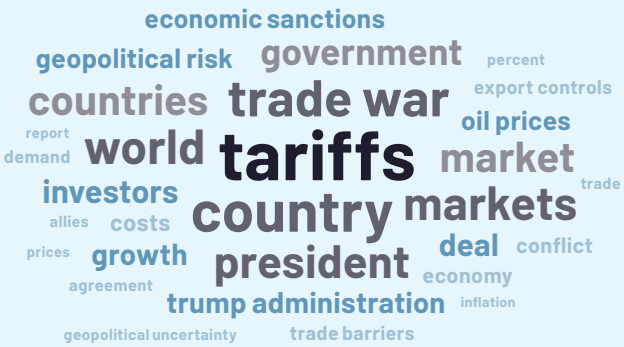


Total mentions - Geopolitical and trade disruption
Jan 2026 - July 2026

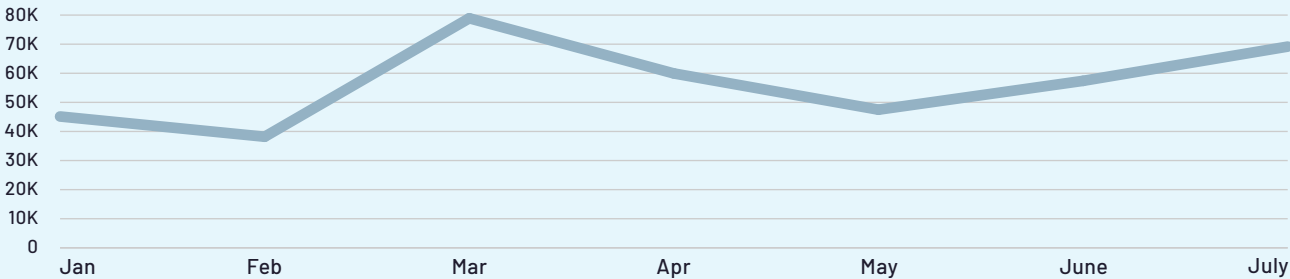


Source: Meltwater

The **geopolitical cluster** was the cleanest of the six. Tariffs, trade war, economic sanctions, export controls, geopolitical risk, oil prices and markets were all directly relevant. The conversation is nonetheless anchored mainly in US trade policy rather than British exposure specifically.

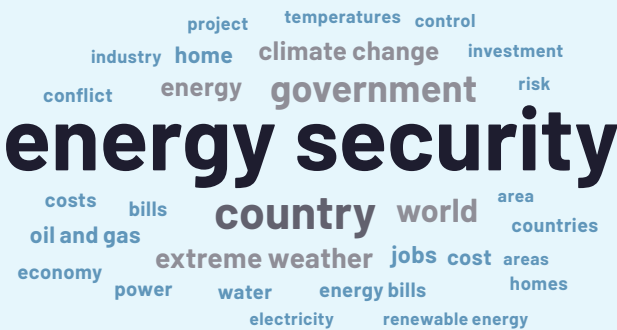


Total mentions - Energy security and critical infrastructure
Jan 2026 - July 2026

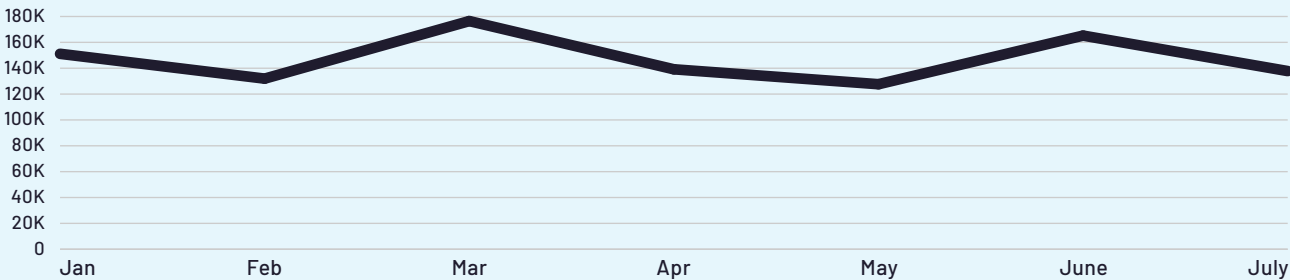


Source: Meltwater

The **infrastructure cluster** was dominated by energy security by a wide margin, followed by climate change, extreme weather, energy bills, electricity, oil and gas, renewable energy and water. Supply chain terminology does not appear in the keyword profile. In practice, this cluster measures energy and climate far more than supply chain resilience.



Total mentions - Misinformation, trust and information integrity
Jan 2026 - July 2026



Source: Meltwater

The **trust cluster** returns fake news, misinformation, disinformation, government, free speech, social media, democracy, truth and police. Corporate reputation terminology is effectively absent. The largest conversation measured across the UK risk landscape is primarily about the integrity of public information, with companies largely absent from it.



Tone

Tone provides a strong indication of how these conversations are developing. The misinformation and trust cluster recorded the most negative sentiment, with economic and workforce discourse improving gradually over the seven months but never leaving negative territory. Energy and infrastructure deteriorated around incidents and recovered between them.

Two clusters followed a different pattern. Cyber discourse began the year as the least negative of the six, deteriorating until a partial improvement in July. It was the only cluster to end the period in a worse position than where it started.

Discussion of AI moved in the other direction, improving significantly over the seven months and approaching neutral by July, even as UK executives reported rising concern.

What this means for companies

The data points to a gap between what business leaders think is important and the risks against which the public assess them. Cyber and technology exposure increasingly define the operational and legal reality, while reputation, trust and cost pressure shape the tone of the environment British companies operate in.

A company communicating about its own resilience is therefore entering a public conversation with limited attention to the subject and a high level of scepticism.

Share of voice by mentions
Jan 2026 - July 2026

Source: Meltwater



Misinformation, trust and information integrity	1.03M	35.7%
Cost of living, taxation, wages and public services	1.02M	35.4%
Energy security and critical infrastructure	391K	13.6%
Geopolitical and trade disruption	189K	6.58%
Cyber and digital operational resilience	160K	5.56%
Artificial intelligence as a business risk	91.7K	3.19%

4. From risks to action

Analysis that combines the government data with business leaders’ and the public’s data suggests a three-tier structure based on how far each risk has already moved from assessment into business consequence.

This shows where pressure is building. The next challenge is deciding how leadership teams should respond. The start point for communications is that organisations need to explain what they are doing, and why, in terms their audiences understand.





Double materiality as a strategic lens

Double materiality assessments can function as a leadership discipline rather than simply a reporting obligation. It requires executives to assess exposure in two directions: the effect of external factors on the company, and the way a company's own conduct impacts the wider world and, therefore, the level of trust bestowed on it.

The UK has made this second dimension more tangible through statutory resilience duties, including incident reporting obligations. Risks that score highly on both dimensions require an integrated strategic response rather than simple monitoring.

Foresight focused on what invalidates assumptions

Over a three-to-five-year horizon, the most useful questions for UK companies are often the ones that test the assumptions behind current strategy. How would operating costs change if statutory resilience duties extended to a wider supplier base? What happens to insurance cost, or even availability, if attacks on the scale seen in 2025 become an annual occurrence?

What happens to demand if consumer confidence remains negative into a second decade? How does labour supply evolve if immigration policy, employment law reform and health capacity constraints continue to compound one another? And what happens to the licence to operate if institutional trust remains near its current low?

Companies that test these assumptions early retain more room to manoeuvre. Conversely, waiting until events provide the answer leaves fewer options available.

Resilience as a leadership capability

It is important to have a strategic corporate approach to resilience, with decisions taken at the highest level to ensure a coherent, company-wide response.

However, this is not yet the case within many organisations. For example, only three in ten UK businesses assign board-level responsibility for cyber risk, according to the Cyber Security Breaches Survey Preparedness Survey.

It is difficult to sustain a concerted response across a company when the responsibility is held exclusively within technical or compliance functions.

Organisations need to have resilience at the highest level.

5. Conclusion

The UK risk environment is changing with risks increasingly interacting rather than arriving as isolated events that can be neatly categorised and delegated to individual functions.

An attack on a supplier can affect national output. Weak household confidence can become a demand constraint. Falling institutional trust can directly affect what companies are able to say credibly about themselves.

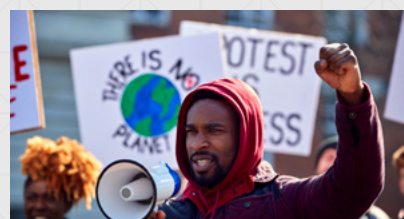
In our research, several findings stand out:



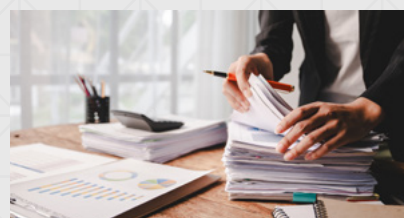
- 1 The risks that British executives rank as immediate differ substantially from the medium- to long-term risks that are identified.



- 2 The risk priorities of British executives differ from those identified by global executives pointing to the fact that there is a unique set of UK issues and pressures that companies are actually experiencing.



- 3 At the same time, public conversation is dominated by issues on which corporates often have limited standing, against a backdrop of low trust and increased scrutiny of corporate behaviour.



- 4 The research suggests that instability will remain part of the operating environment, making the ability of companies to plan and adapt before strategic options narrow increasingly important.



- 5 Recent extreme weather events have renewed attention on the economic consequences of a warming world, highlighting the ongoing influence of climate change on international stability and corporate decision-making.

Call to action



The UK Government has raised its expectations of business' resilience and adaptation planning faster than many companies have strengthened their own preparedness.



Rising expectations around governance, transparency and contingency planning are making resilience a core business imperative.



Organisational readiness will soon become a regulatory requirement rather than a voluntary undertaking.



Environmental concerns continue to shape the strategic landscape, with the focus shifting from prevention to adaptation. Companies are expected to demonstrate measurable progress around adaptation, with greater emphasis on delivery and tangible outcomes rather than disclosure in isolation.

6. The Leidar adaptation and resilience approach

Leidar works with organisations to turn disruption into resilience and resilience into strategic trust. The approach is structured around six questions leadership teams need to answer before acting:

- ? *What external forces are affecting our ability to operate?*
- ? *Where are we exposed across climate, nature and biodiversity, energy, water, AI, data, geopolitics, social shifts and regulation?*
- ? *Who are the relevant stakeholders, and have they changed?*
- ? *How can resilience move beyond risk management and support strategic advantage?*
- ? *What narrative can align investors, employees, policymakers, clients and partners?*
- ? *And what needs to change in company culture for adaptation to become meaningful in practice?*

The work program is organised across different stages. It begins by scoping the resilience focus across geography, products and services, supply chains and objectives, and it identifies issues and risks through materiality analysis and a SWOT review. It then prioritises risks and opportunities according to severity, horizon, financial impact and stakeholder relevance. Finally,

it supports the organisation in translating these findings into strategy, narrative, and stakeholder outreach including stakeholder mapping and a defined outreach action plan.

The abiding principle is that it is up to the communicator to communicate, not the audience to interpret. We all lead busy lives and do not listen unless the message is clear and relevant.

Phase 1: Adaptation and resilience analysis

This begins with a boundary-scoping exercise to determine which factors, geographies and supply chain tiers are in scope. This has relevance in the UK given that two of the most costly national incidents of the past two years entered through the private sector. The analysis then moves through double materiality across climate and nature, geopolitics, defence and intelligence, and technology and AI, followed by a SWOT review and a deeper examination of acute and chronic risk. It concludes by prioritising the risks and opportunities that should inform strategy.

Phase 2: Action plan and roadmap development

This translates the analysis into stakeholder mapping, narrative development grounded in evidence, foresight through scenarios and trigger dashboards, and a practical implementation and engagement roadmap. It can also cover advocacy and coalition building, market and investor materials, crisis protocols, capability development, and a reporting strategy for a regulatory environment in which resilience disclosure is increasingly moving from voluntary practice towards formal requirement.

The **Leidar Resilience Dashboard** supports both phases by looking at exposure through a risk ranking and heat map, institutional preparedness through an adaptation maturity score, future adaptation through scenario resilience scoring, stakeholder capital through a trust and influence map, and strategic response through priority actions, quick wins, strategic bets and capability gaps.

References

- Agriculture and Horticulture Development Board. (2026). Harvest progress report (2nd report of 2026). AHDB.
- Allianz Commercial. (2026). Allianz risk barometer 2026. Allianz Commercial. commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html
- Allianz Trade. (2026). UK risk barometer 2026. Allianz Trade. allianz-trade.com/en_GB/insights/economic-research/2026-uk-risk-barometer.html
- Cabinet Office. (2026, July 14). National risk register 2026. HM Government. gov.uk/government/publications/national-risk-register-2026
- Climate Change Committee. (2026). Adaptation progress reporting. Climate Change Committee.
- Cyber Monitoring Centre. (2025a). Statement on ransomware incidents in the retail sector [Press release]. Cyber Monitoring Centre.
- Cyber Monitoring Centre. (2025b). Statement on the Jaguar Land Rover cyber incident [Press release]. Cyber Monitoring Centre.
- Department for Business and Trade. (2026). Global supply chains: A foresight report on risk and resilience. UK Government.
- Department for Science, Innovation and Technology, & Home Office. (2026, April 30). Cyber security breaches survey 2025/26. GOV.UK. gov.uk/government/statistics/cyber-security-breaches-survey-2025-2026
- GfK. (2026). Consumer confidence barometer. GfK, powered by NIQ.
- Ipsos. (2026). Issues index. Ipsos. ipsos.com/en-uk/topic/issues-index
- Marsh. (2026). UK business risk report 2026. Marsh LLC.
- National Cyber Security Centre. (2025). Annual review 2025. NCSC.
- National Farmers’ Union. (2026, August 11). NFU calls for urgent action as drought expands across England [Press release]. NFU.
- NatCen Social Research. (2026). British social attitudes: Trust and confidence in Britain’s system of government. NatCen.
- World Economic Forum. (2026). Global risks report 2026. World Economic Forum. weforum.org/publications/global-risks-report-2026/

Leidar is a leadership and corporate affairs consultancy that helps clients set their course, navigate and communicate effectively.

This is Leadership Navigation.

We hope you have found this report useful.

If you would like further detail about the findings, or more information, please contact:



Peter de Graaf
peter.de.graaf@leidar.com
2 Kingdom Street,
London W2 6BD



Charlie Pryor
charlie.pryor@leidar.com
2 Kingdom Street,
London W2 6BD



Lukasz Bochenek
lukasz.bochenek@leidar.com
Rue Muzy 7
1207 Genève

leidar.com

in Leidar

Rue Muzy 7,
1207 **Geneva**
Switzerland

Rue du Sceptre 57A
1050 Ixelles, **Brussels**
Belgium

2 Kingdom Street,
London W2 6BD
United Kingdom

Grev Wedels Plass 4,
0151 **Oslo**
Norway

JAFZA One, Tower A
PO Box 35608, **Dubai**
United Arab Emirates

991 Bukit Timah Road
#05-09, 589630
Singapore

1500 K Street, NW, 2nd Floor
Washington, DC 20005
United States of America

14 Penn Plaza 225 West 34th
Street, **New York, NY** 10122
United States of America

About Leidar

Headquartered in Geneva with offices in London, Brussels, Oslo, Dubai, Singapore, Washington, DC and New York, we mainly work with businesses and organisations that operate on a global scale. We understand how to develop and deliver their messages to a wide internal and external stakeholder audience and how to leverage business opportunities in a rapidly changing political landscape.

Our clients include companies, both publicly listed and private, industry groups as well as international organisations and NGOs, across all sectors.