STRENGTHENING OUR ECONOMIC RESILIENCE

Building an effective partnership between business and government

Contents

Foreword

We live in an era marked by unprecedented threats and uncertainties. From geopolitical tension to pandemics, and from technological advancements to climate change, these shocks have underscored a clear but challenging necessity for robust and adaptive systems capable of withstanding, reacting to, and recovering from national crises. Businesses large and small are often at the coalface, fronting much of the uncertainty and solutions. This report and its recommendations, co-created with industry, government and resilience-focused stakeholders, outlines how partnership between the private sector and the government can advance our shared goal of resilience.

Governments past and present have undertaken welcome steps to develop safeguards. We were delighted to see the new Government take early and decisive action to launch a review of National Resilience and embed resilience as a core pillar of the Industrial Strategy Green Paper, highlighting their commitment to a proactive and holistic approach. Resilience and futureproofing are key components of the government's ambition for economic growth.

However, to truly achieve this goal and seize the growth prizes on offer in the UK, we must work together to be better prepared for shocks. When governments provide strategy and vision, setting out the big bets we want to make together, businesses can fill the gaps through industry expertise. Their ability to invest, compete, and innovate make them an indispensable partner. But they need help: only 29% of our members feel they have invested sufficiently in resilience. With a difficult investment environment continuing, we must also look to work together to solve this puzzle.

Partnership is, and has always been, at the heart of what the CBI does. Effective engagement, honest sharing of challenges, and collaborative solutions, will be how the nation's resilience is secured. The pandemic revealed both a vulnerability in the interconnectivity of the economy but also shone a light on the complexity of its supply chains. Nevertheless, remarkable examples of businesses stepping up to support the national effort emerged. Together, with government, we navigated this global crisis and demonstrated the power of partnership to tackle threats.

This report urges government and business to consider economic growth and economic resilience as two sides of the same coin. By working in partnership on our shared goal, we can build an economy where its inherent adaptability is not just a response to adversity, but an enabling asset in our mission for sustainable growth

JFoster

John Foster
Chief Policy and Campaigns Director, CBI

Foreword

We live in a volatile and uncertain world: the international situation is turbulent and threatening. We have seen significant disruptions to supply chains in the last couple of years, and the experience of COVID reminds us how rapidly the norms of society can be disrupted. But pandemic is only one of the 89 risks that feature on the Government's National Risk Register, which deliberately excludes chronic or slow-burn risks like climate change, anti-microbial resistance and AI.

Every business needs to take this environment into account in their planning to ensure that they are prepared for and resilient to whatever may happen – because business relies on the nation to be prepared and resilient. Without that foundation, economic growth is fragile and unsustainable. Resilience must be a key government responsibility.

However, it is a shared challenge: business needs the country to function, to be prepared and resilient; but so too does the nation need business to be prepared and resilient. Every business is mutually dependent on the preparedness and resilience of its suppliers, its customers and its neighbours. This is why successive governments have talked about the need for whole-of-society resilience. Resilience must be part of society's fabric: it cannot just be a question for national government, but preparedness and resilience must be designed into every community and into every business. This is why the CBI sits on the panel of Commission members at the National Preparedness Commission.

If we can make every level of government, every community, and every organisation and business more resilient, we can create a sort of herd immunity for a society better able to address future crises and threats – whether it is a new pandemic, a massive cyber-attack or climate change. As a nation, we need to be better prepared for all the hazards that might affect us, not only to protect us for the future but to provide the foundation for long-term growth and success. This requires a true partnership between government and business with a shared agenda. The CBI's report, *Strengthening our National Resilience*, marks a critical contribution in identifying what is needed to build that shared agenda.

Toby Harris

Lord Toby Harris
Chair, National Preparedness Commission

Executive Summary

While the pursuit of economic growth must continue to be our mission, ensuring resilience and growth are seen as two sides of the same coin is paramount

Through globalisation, the UK's interconnectedness with the global economy has brought significant benefits for businesses and consumers alike. Recent events have, however, demonstrated that this interconnectivity can have a profound impact on the UK economy when negative unforeseen shocks occur.

The pandemic, global conflict, and disruption in the Red Sea and other critical trade vessels have demonstrated the impact of global events on UK supply chains and made it necessary for industry to adapt. At the same time, protectionism and geopolitical tensions are on the rise, and businesses and governments across the globe have had to become increasingly alive to risks such as cyber security, food security as well as climate change and energy security.

These events have demonstrated that resilience is a vital precursor to achieving sustainable growth. A review of the UK's resilience is expected to be published by the Cabinet Office in 2025 following this year's covid inquiry report which highlighted broader lessons. The UK's national resilience therefore embodies a burning platform for government and business and provides an imperative for both to work in lockstep to ensure resilience sits alongside the UK's growth mission and new Industrial Strategy.

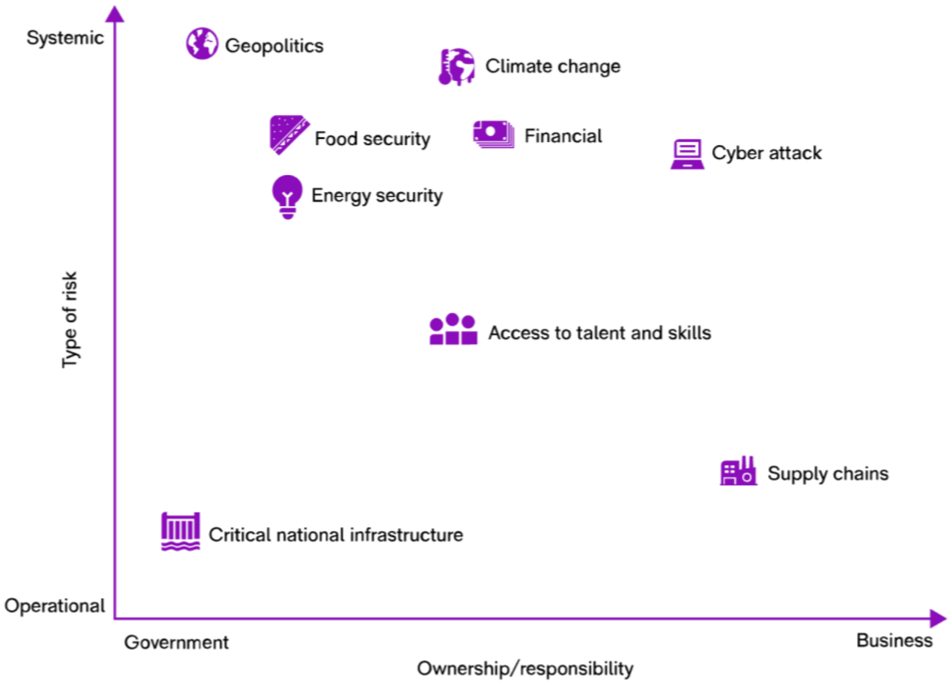
Navigating unforeseen shocks and unknown risks requires a coordinated approach between government and industry, central to any resilience strategy

The broad range of risks facing the economy need to be understood by both government and business. While both agents have a role to play in strengthening the UK's resilience, ownership and responsibility will be determined by the type of risk as well as the expected economic and societal impact. But for the UK to truly be resilient to shocks, a coordinated approach between business and government is needed.

When it comes to systemic risks, governments have a critical role to play in ensuring the impact to the economy and to society is minimised, but this should be supported by effective dialogue between industry. Installing the appropriate architecture to enable this is therefore key so businesses and governments can respond at pace when unforeseen shocks occur.

But this is not just about what more government can do. Businesses should proactively seek to embed resilience at the core of their operations by taking the appropriate steps that will help them to survive not only systemic shocks but also shocks unique to their sector or business. According to recent CBI surveys, only 29% of businesses feel they have sufficiently invested in building resilience to economic shocks, highlighting a significant gap in resilience planning. Government can help with this by providing the appropriate policy framework and incentives to promote behavioural change. **Figure 1** aims to provide a high-level representation of the role of business and government in building a resilient nation.

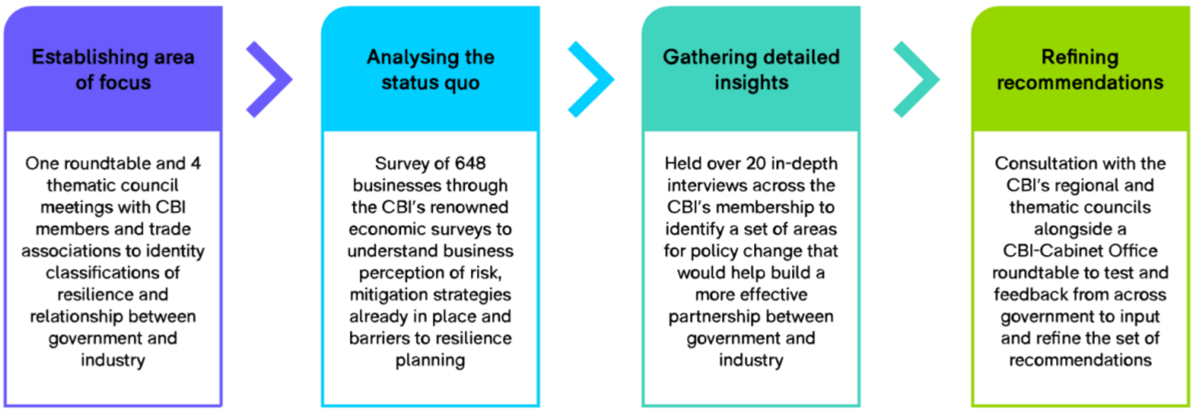
Figure 1: Representation of the role of government and business in resilience



Source: CBI assessment based on member discussions

Building resilience across our economy has risen up the agenda in our mission to make the UK a more competitive place to do business. The CBI welcomes the early announcement of a resilience review by the Chancellor of the Duchy of Lancaster, the Rt Hon Pat McFadden MP, and business is committed to further entrenching this across the UK economy in collaboration with Government. This policy paper aims to support this review by leveraging the expertise and experience of the business community across the whole economy. It has been developed in extensive consultation with both CBI members and the relevant departments across government. **Figure 2** provides an overview of the business engagement that has shaped this report.

Figure 2: Extensive member consultation



Summary of recommendations

Being clear about government's role to address systemic risks

1. The National Risk Register represents a comprehensive central bank of potential risks to the resilience of the economy and broader society. However, with 89 risks identified, it represents a detailed, granular download as opposed to a strategic overview. Industry thrives when it has clear, consistent steers from government. With the Industrial Strategy designed to provide a ten-year vision for where the UK can compete to win on the global stage, it is important that the Government provides equivalent clarity to businesses about the risks to resilience. With the Government currently consulting on the Industrial Strategy, this represents an opportunity for the Government to identify the major, strategic risks to resilience that business will face over the next decade.
2. As part of the government's recent Green Paper on the UK's Modern Industrial Strategy and through the resilience review, the government should work with industry to develop an effective 'operating model' for how government decision making can support the resilience objectives of the Industrial Strategy. The Green Paper puts forward a *Theory of Change* to illustrate the logical relationships between Industrial Strategy policies and growth. The Government should look to build on the *Theory of Change* proposal to encompass a more formal 'operating model' that can be deployed to address the tension within Whitehall that can occur between investment facing departments and those that are more security focused. Developing the *Theory of Change* to account more explicitly for resilience will help government to effectively prioritise policy decisions and build the appropriate business engagement architecture that not only achieve the government's growth ambition, but also achieve the economic security objectives as set out in the Industrial Strategy green paper.
3. Build on existing engagement architecture to ensure business can input into UK foreign policy priorities given the implications for their operations. Industry understands the use of sanctions, international agreements and other foreign policy tools but would like to be more involved in the conversation. Building on the successful new ways of working established during the development of the sanctions regime and deploying this strategically in more areas will increase business understanding of the decisions made by government and help to minimise uncertainty. Industry is a crucial component of the UK's soft power due to its unique international relationships. Hardwiring cooperation with the government, including FCDO and relevant departments, as well as the use of specific fora for addressing and managing risks is critical to leverage this power, and ensure dialogue with business in this context.

Harnessing collective efforts with business

4. As part of the wider governance on resilience, the government should consider the role and remit of a new risk committee that brings together senior cross-Whitehall resilience leads (from across specialisms including national security and economic growth), as well as senior representatives from the business and academic community. This committee would act as the overarching body on resilience, with sector/ topic specific bodies created on an ad-hoc basis where necessary. The remit of this committee would be to monitor and develop mitigation strategies for current and emerging risks.
5. Building effective public-private partnerships is critical to ensure that businesses across the economy are protected against risks. In some areas, the UK insurance industry has been able to develop efficient solutions already. Adapting these successful public-private systems to new risk areas, including security issues, and simultaneously updating insurance schemes is essential to building a resilient economy. The government should continue working in partnership with the insurance industry to deploy effective schemes, widening their scope and therefore helping companies to be more resilient.

Helping businesses build operational resilience

6. The government's review of national resilience alongside the Industrial Strategy should identify where market failures exist in the uptake of resilience-based investments, and where there are information asymmetries. This should involve the following:
    - Build upon existing training solutions (apprenticeships, bootcamps, etc) to deliver more flexible and modular options, utilising the Growth and Skills Levy to act as an incentive to employer investment in skills;
    - Exploration of how the new Resilience Academy can act as a forum for information sharing across sectors;
    - Examination of whether there is a market failure in accessing finance for resilience purposes and where the funding system could support firms to both build resilience and to access the cash needed to cope with shocks as and when they arise. The CBI stands ready to investigate this further to ensure all businesses are able to access the finance they need to build their operational resilience; and
    - Through the resilience review, continue to work with stakeholders to establish a consolidated mechanism for timely information sharing with businesses about upcoming risks and potential consequences. The CBI stands ready to work more closely with government on ensuring the most effective mechanisms for information sharing with business in both directions.

Being clear about government's role to address systemic risk

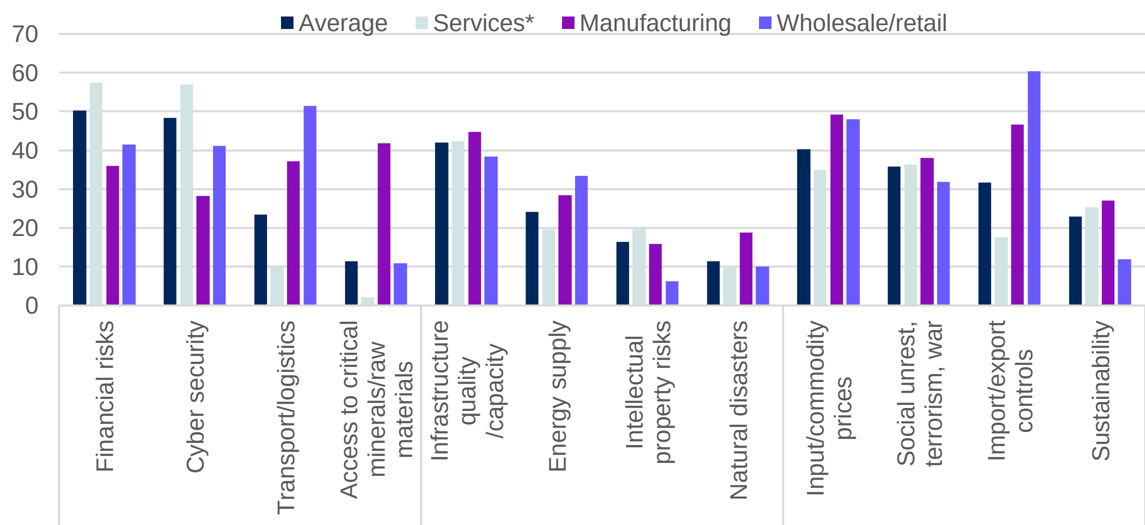
Setting a clear overarching strategy can help implement practical measures at pace and send the right signal to businesses and global partners

Recent events, including the pandemic and global conflicts, together with new threats such as cyber, have shone a spotlight on the resilience agenda, with several policy initiatives and strategies already taken forward in response.[1] Earlier this year, the publication of the Covid Inquiry report highlighted the broader lessons for resilience and resulted in the Minister announcing a Cabinet-level review of national resilience.[2]

For business, these initiatives are setting the right direction on resilience both from a signalling perspective (that the Government is taking a long-term view) and from a practical standpoint (with useful policy levers to help business build resilience). However, anecdotal evidence suggests these initiatives are often siloed across departments, and within sectors, and businesses struggle to understand how these initiatives fit together at a strategic level.

Furthermore, as shown by **Figure 3**, perception of risk differs by sector.[3] Network-related risks feature highly for consumer, professional & business services firms, whereas geopolitical risks feature more prominently for manufacturers, logistics and distribution firms. This suggests businesses think differently about risk depending on their sector and business model, which is likely resulting in inconsistencies in resilience planning and mitigation strategies.

Figure 3: External risks to business operations/supply chains (Next two years, % of respondents, weighted average vs sectors)



Source: Aggregation of data from different CBI surveys of June 2024.
* Private non-financial services, excluding wholesale/retail.

Recommendation 1: The National Risk Register represents a comprehensive central bank of potential risks to the resilience of the economy and broader society. However, with 89 risks identified, it represents a detailed, granular download as opposed to a strategic overview. Industry thrives when it has clear, consistent steers from government. With the Industrial Strategy designed to provide a ten-year vision for where the UK can compete to win on the global stage, it is important that the Government provides equivalent clarity to businesses about the risks to resilience. With the Government currently consulting on the Industrial Strategy, this represents an opportunity for the Government to identify the major, strategic risks to resilience that business will face over the next decade.

A focus on Supply chains

Supply chains are changing and becoming more fragmented across the global economy. Last year, Make UK reported that 80% of manufacturers identify supply chain vulnerabilities as a significant strategic risk.[4] The World Economic Forum also reports that 57% of businesses experienced significant disruptions in their supply chains over the past year.[5]

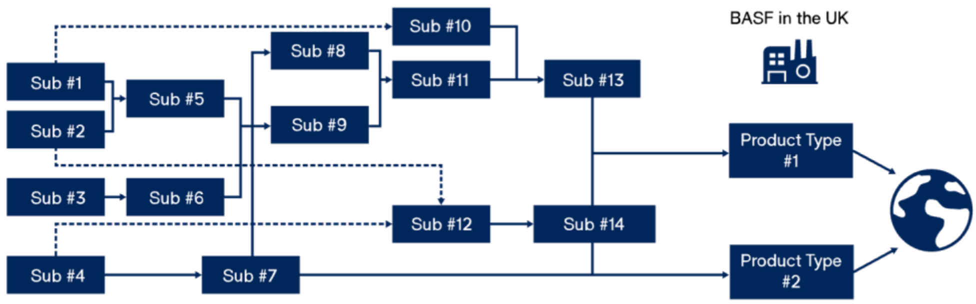
Strategies to enhance supply chain resilience include diversifying suppliers, increasing transparency and investing in advanced technologies for real-time monitoring and risk management. Protecting domestic supply chains is also critical to this to ensure production can be retained and expanded in the UK. While there is no 'one-size fits all' solution to future-proof supply chains, the CBI recognises that there are several factors which underpin a clear supply chain strategy. These challenges are exacerbated for SMEs who often struggle with analysing supply chain vulnerabilities compared to larger organisations with more resources.

Case Study: BASF on supply chain resilience in the chemical sector

BASF operates in the chemical manufacturing sector with six sites in the UK. As a global company with its largest production footprint in Europe, it is one of the largest suppliers of raw materials to various industries in the UK, including agriculture, automotive, chemicals, construction, energy, and pharmaceuticals. The chemicals manufacturing industry is foundational, meaning it provides solutions to the industrial transformation needed for net zero: chemicals are needed for the deployment of most green technologies, from wind turbines and electrolysers to advanced recycling and sustainable agricultural practices.

BASF view resilience in terms of their supply chain. Chemicals value-chains are highly complex and often spanning across different geographies: the manufacture of a single chemical product can be multi-layered and as such, there is a reliance throughout the value-chain for robustness, competitiveness and efficiency.

To illustrate this, BASF conducted a value-chain analysis for a range of products manufactured at one of its six UK sites. At this specific site, the finished chemical product sits at the sixth level of the value chain. This means that for the site's UK operations to be timely and cost-effective, a synthesis path containing at least fourteen pre-cursor chemicals over five 'value-chain levels' is required.



Replicated across key industries, this shows how resilient chemicals value chains are key for realising the UK's net zero target and growth ambitions.

As part of economic resilience in the UK, a more targeted approach to the chemicals industry would help them to navigate challenges and seize opportunities to drive economic growth across the country. This should be translated, for example, in leveraging sector expertise within a Chemical Industry Council, as the chemical industry is not fully integrated into government's policies for resilience and its interconnection to other sectors is often underestimated.

The CBI welcome the recent Industrial Strategy Green Paper which has resilience as one of the four key pillars. Strengthening the UK's resilience will be key to the success of any Industrial Strategy and the UK's growth mission. While the economic security objectives set out are the right ones, we believe the strategy should also reinforce the need to consider growth and resilience together, ensuring policy decisions are viewed through both a growth and resilience lens and coordinated across government departments.

This is important for:

- Enabling government and business to understand the interconnectedness of risks and mitigation strategies;
- The creation of consistency across government departments and encouraging better coordination between security experts and officials focused on economic growth;
- Moving away from a siloed strategy, understanding the cross-sector implications of decision-making, and allowing businesses and other external stakeholders to identify where their expertise can be leveraged and how they need to be thinking about their own operational resilience; and,
- Sending an important signal that the UK takes resilience seriously thereby strengthening our competitive advantage as a place to do business.

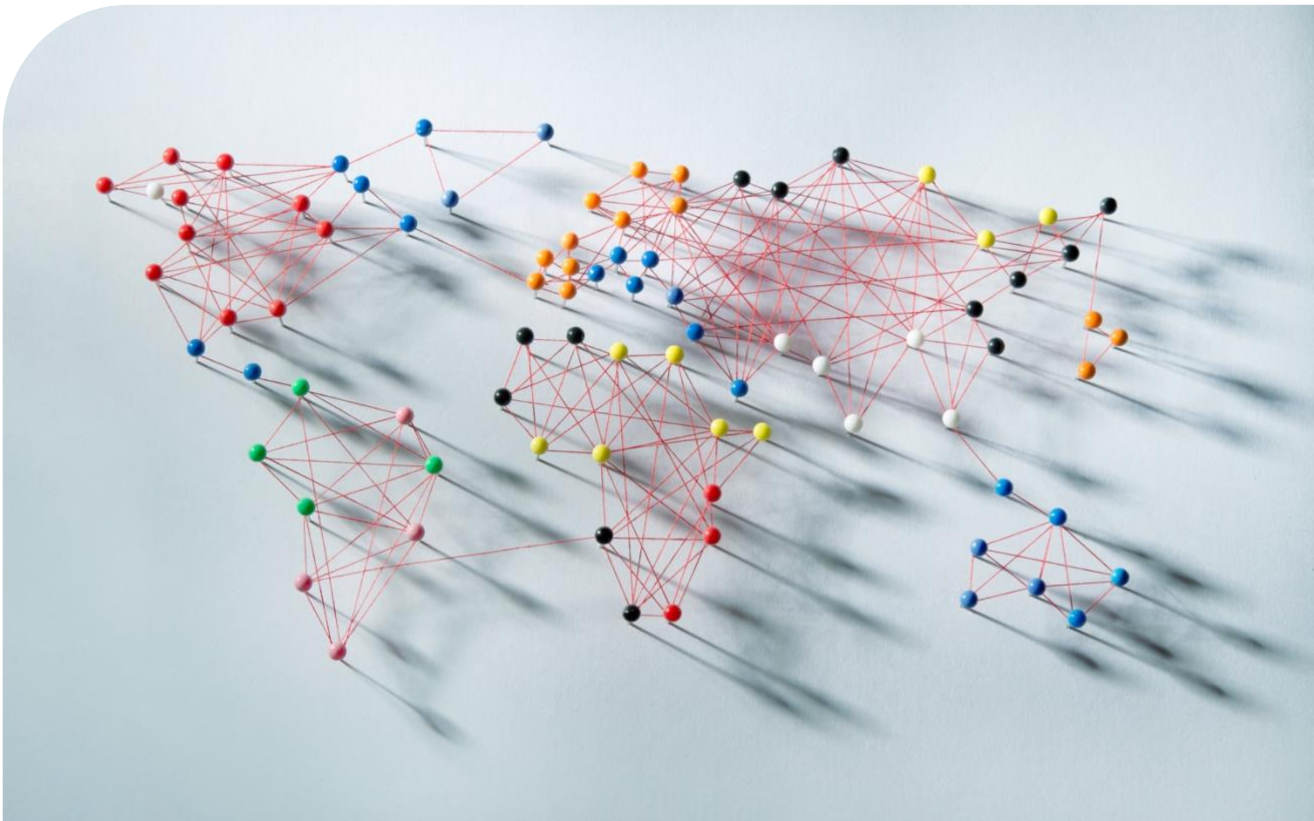
Recommendation 2: As part of the government's recent Green Paper on the UK's Modern Industrial Strategy and through the resilience review, the government should work with industry to develop an effective 'operating model' for how government decision making can support the resilience objectives of the Industrial Strategy. The Green Paper puts forward a *Theory of Change* to illustrate the logical relationships between Industrial Strategy policies and growth. The Government should look to build on the *Theory of Change* proposal to encompass a more formal 'operating model' that can be deployed to address the conflict within Whitehall that can occur between investment centred departments and those that are more security focused. Developing the *Theory of Change* to account more explicitly for resilience will help government to effectively prioritise policy decisions and build the appropriate business engagement architecture that not only achieve the government's growth ambition, but also achieve the economic security objectives as set out in the Industrial Strategy green paper.

With geopolitics cited as the main global economic risk for the business community, hardwiring cooperation between government will be more important than ever

Tensions between global actors are on the rise, from war in Europe and the Middle East to heightened rhetoric between China and Taiwan - events which are largely out of the control of business. According to a recent survey by Oxford Economics, geopolitical tensions were seen as the number one risk to the global economy over the next five years, cited by almost 80% of respondents.[6] Similar concerns have been raised consistently through the CBI's member engagement.

However, businesses have cited there is very little proactive engagement on foreign policy initiatives, resulting in government and industry reacting to events with little preparation time. For example, when the war in Ukraine began, government needed to quickly assess the potential impact on supply chains, and businesses were unsure on whether, and how, sanctions would be implemented. Businesses recognise the role of sanctions as an important element of UK foreign policy, but reported not being effectively plugged into the discussions that would ultimately have implications for their operations.

Businesses recognise that when it comes to matters of national security, it is right that government take the lead. Involving business insight and input at the earliest possible moment can ensure that those decisions are taken with full consideration about the impact on the economy. Furthermore, in some cases, the outcomes of geopolitical crises are not entirely unpredictable; such as a Middle East oil embargo, the closure of sea lanes or a major overseas port, or sanctions on China over tensions with Taiwan. In those situations, scenario planning between government and industry would be helpful to help troubleshoot and mitigate against any unintended consequences.



We believe the Government can help to minimise the economic impact of geopolitical developments through the following steps:

- First, notification of emerging risks as early as possible, with recognition of the confidential nature of the information exchanged. The National Risk Register is a good starting point with a good level of granularity, but including more details on scenario planning and the actions for business and government would be beneficial.
- Second, an assessment of the potential exposure to the economy and where impacts can be reduced, working in collaboration with business.
- Third, to ensure UK foreign policy successfully balances economic and national security interests. Bringing together security and economic experts from across government and industry will be central to this. The UK's relationship with China is front of mind for many businesses given its implications on supply chains and trade.
- And finally, continue creating synergies and enhancing cooperation with key partners, such as the EU and the US, to address global challenges. The UK-EU collaboration on critical minerals, and economic cooperation with the US under the Atlantic Declaration signed by the previous administration, were cited as good examples of this cooperation.

Recommendation 3: Ensure business can input into UK foreign policy priorities as these have implications on their operations. Industry understands the use of sanctions, international agreements and other foreign policy tools but would like to be more involved in the conversation. Building on the successful new ways of working established during the development of the sanctions regime and deploying this strategically in more areas will increase business understanding of the decisions made by government and help to minimise uncertainty. Industry is a crucial component of the UK's soft power due to its unique international relationships. Hardwiring cooperation with the government, including FCDO and relevant departments, as well as the use of specific fora for addressing and managing risks is critical to leverage this power, and ensure dialogue with business in this context.

Harnessing collective efforts with business

Setting the right architecture to ensure effective dialogue between government and business

While the Cabinet Office's Resilience Forum was a key part of the engagement architecture to enable industry to participate on matters of national resilience, the CBI believe an even closer partnership could be formed to continually monitor and mitigate risks to the UK economy. Areas on which the Resilience Forum could be improved include:

1. The rotating membership structure was beneficial to ensure the most appropriate experts are in the room, but could have contributed to the siloed nature of many of the policy initiatives and risked ignoring the interconnectedness of many risks.
2. Topic-based discussions on a quarterly basis fulfilled the need for a more formal structure to enable the right people to come together to solve a problem, but reduced the ability for government and business, and other resilience experts, to collectively discuss risks closer to real time.
3. Cabinet Office should continue using their role as a cross-Whitehall convener to ensure that key departments are involved in discussions as appropriate, so business has a single gateway for inputting resilience insights into government.

An example of a successful model is the UK Finance and Bank of England CMORG initiative, which was established to effectively bring industry expertise into conversations relating to the resilience of the financial services sector.

Case Study: UK Finance/BoE CMORG initiative

- The Cross-Market Operational Resilience Group (CMORG) is a strategic partnership structure between UK Finance and the Bank of England, supporting industry in enhancing sector resilience. It is often cited as a prime example of how industry collaboration can be harnessed to collectively monitor and mitigate risks.
- It leverages the expertise of various specialist industry groups to design and implement resilience strategies, focusing on areas such as cyber security, third-party risk management, and business continuity.

An engagement structure like this would allow government to better assess the knock-on impact of emerging risks, identify where industry can help to mitigate these, and increase the awareness of industry to these risks. This will equip businesses with the information needed to better manage their own operations in response.

In developing any engagement architecture, consideration should be taken at a national, regional, and local level. This will be particularly important in the context of devolution. The Netherlands has been cited as international best practice when it comes to government-business engagement.

Recommendation 4: As part of the wider governance on resilience, the government should consider the role and remit of a new risk committee that brings together senior cross-Whitehall resilience leads (from across specialisms including national security and economic growth), as well as senior representatives from the business and academic community. This committee would act as the overarching body on resilience, with sector/ topic specific bodies created on an ad-hoc basis where necessary. The remit of this committee would be to monitor and develop mitigation strategies for current and emerging risks.

Leveraging private sector expertise to further bolster the existing capabilities of the UK government

While government have a range of resilience and security experts across departments, the private sector also has a wealth of expertise to draw upon which is currently not being fully utilised.

For many businesses, risk and security are their core business model. For example, the insurance sector exists to mitigate and manage risk on behalf of businesses. Where the impact of a shock would be too large for either government or business to carry alone, public-private partnerships have been successful in managing fallout.

Pool Re is an example of an effective public-private partnership, covering £2.2 trillion of UK based assets including businesses of all sizes against terrorism, and operating with an unlimited HMT loan facility. Likewise, Flood Re re-insurance scheme that protects households against flooding, provides a successful model of coordination between the UK insurance industry and the government.

A spotlight on cyber and the role of cyber insurance

Insurance is an effective economic security tool, acting both to reduce the likelihood and impact of potential threatening cyber incidents, as well as supporting and accelerating the return to 'normal' following an attack. The damage from an attack is most easily reversed when supported by the swift injection of capital to finance remediation—from crisis counsel and information technology forensics to simply being able to pay staff and avoid redundancies or even bankruptcy while unable to trade or transact, particularly for small businesses.

Access to finance poses one of the biggest challenges when businesses are looking to bolster their economic resilience. The phrase "cash is king" underscores the critical importance of liquidity in navigating crises. More agile insurance schemes, particularly in the realm of cybersecurity, can further enhance national resilience by focusing on systemic risks. These schemes not only provide financial coverage but also emphasize proactive measures such as training and information sharing. By investing in these areas, insurance can help businesses and governments better anticipate and mitigate the impacts of cyber threats

Recent OECD research on the savings from implementing a catastrophe risk insurance program estimates that a 1% increase in insurance coverage can reduce recovery time by nearly 12 months and decrease post-disaster government expenditure by 22% of the damages.

Cyber now presents a new challenge where both insurance and cyber security expertise have a crucial role to play, but this will only be successful if working in close collaboration with government. The US Joint Cyber Defence Collaborative has been cited as best practice business and government collaboration on cyber security.

Case study: How S-RM's intelligence-led risk management approach supports organisational resilience

The traditional approach to risk management is resulting in disjointed information and advice serving as input for the decision-making process at C-level. S-RM support clients through an integrated, intelligence-led approach to risk management and organisational resilience.

This starts with an understanding that the external landscape that organisations operate in cannot be split into discrete and unrelated threat categories. Threats stemming from the geopolitical landscape such as political instability, sanctions, human rights failings, climate change and macro-economic pressures, must be understood both in conjunction with threat drivers in the digital ecosystem, such as corporate and state-led espionage, technological disruption and cyber-attacks, and with the drivers of organisational threats, such as supply chain disruptions, activism, regulatory changes and sustainability, to name a few. S-RM bring both their intelligence, sustainability and cyber security consultants together, taking a step-by-step and integrated approach to supporting organisational resilience.

In the first instance, comprehensively mapping the threat landscape helps organisations to anticipate emerging threats and refine their intelligence requirements. Following from this, specific scenario exercises allow for organisational preparedness for likely as well as less likely but potentially high-impact outcomes, supporting internal planning, risk management and crisis response procedures. Finally, having refined the organisation's intelligence requirements and critical scenarios, bespoke ongoing monitoring systems focusing on tactical, operational and strategic threats, allow for a timely response to immediate threats as well as horizon scanning for indicators of shifts with strategic implications.

Beyond public-private partnerships, the government can also benefit from the products and services created by the private sector, leveraging their expertise to improve the defences of public sector organisations from a national security perspective. Innovative products and services are crucial in the pursuit of greater resilience for public sector organisations and businesses across the UK. The private sector has the solutions – whether that's using AI to efficiently map an entire company's supply chain and any potential ESG implications, or maximising uptake of cutting-edge cyber security products.

With cyber cited as one of the biggest risks to the global economy, the expertise of the cyber security sector has never been more important. The CBI welcomes current government initiatives to help businesses protect themselves against the most common cyber threats. The announcement of a Cyber Security and Resilience Bill which aims to strengthen the UK's defences and ensure that more essential digital services are protected, in addition to putting regulators on a strong footing to ensure essential safety measures are being implemented, play an essential role in safeguarding the UK's critical national infrastructure by placing security duties on industry involved in the delivery of essential services.

Recommendation 5: Building effective public-private partnerships is critical to ensure that businesses across the economy are protected against risks. In some areas, the UK insurance industry has been able to develop efficient solutions already. Adapting these successful public-private systems to new risk areas, including security issues, and simultaneously updating insurance schemes is essential to building a resilient economy. The government should continue working in partnership with the insurance industry to deploy effective schemes, widening their scope and therefore helping companies to be more resilient.

Helping businesses build operational resilience

Ensuring resilience is a boardroom priority will help place resilience higher on the agenda for business

Strengthening the UK's national resilience is not only a duty for government. The business community have a crucial role to play to build their operational resilience to ensure they can withstand future shocks to their operations, helping to minimise the wider impact on the economy and on society.

As we navigate an increasingly connected and volatile environment, resilience is becoming even more crucial for business. A recent CBI survey showed that the two biggest risks to business operations and supply chains both relate to key external networks, with 50% of firms citing financial risks and 48% citing risks around cyber security.[7] And these risks are becoming more prominent to business operations, with 58% of firms citing risks have increased over the past two years.[8]

However, the same surveys show that almost two thirds of firms (64%) are either working to improve crisis management capabilities or feel they have sufficiently invested already, which leaves a sizeable minority of firms that are taking no action.[9] This underlines the importance of making resilience a boardroom priority for all businesses, regardless of their size or sector. On the one hand, business leaders should take increased ownership of strengthening resilience across their company operations and governance, promoting a behavioural change. On the other hand, the government should spread adequate level of information about potential and actual economic shocks, providing guidance to industry board members.

Resilience is now a competitive differentiator. Businesses that invest in resilience can better navigate uncertainties and maintain operations during crises. When surveyed, CEOs globally often list geopolitical developments, cyber security, supply chain continuity, sustainability and economic shifts as the greatest concerns facing their organisation.[10] This is hardly surprising given the sheer pace and unpredictability of global events of recent years.

The growing interconnectedness of drivers of organisational threats further complicates the many moving parts that executives must track, with geopolitical developments in one part of the world resulting in operational disruption, cyber security risks and economic shocks in another. However, even in this context and amid a growing sense of global uncertainty, many organisations continue to deal with risks in silos, leaving them unnecessarily exposed or over-focused on some issues over others. For this reason, many businesses believe that risk needs to be part of the corporate mindset, and not purely a box ticking exercise.

Identifying and addressing the top barriers holding back investment is crucial to unlocking the necessary investment to build a resilient nation

While the desire for firms to build their operational resilience exists, they face multiple barriers when it comes to investing in resilience, with the biggest barriers cited in CBI surveys as lack of appropriately skilled staff, access to finance and difficulties assessing risk.

Lack of appropriately skilled staff

Factors around the labour market including accessing skills and demographic changes have been flagged as both a risk in itself and a barrier to building resilience across the UK. According to CBI surveys, a lack of appropriately skilled staff was seen as the biggest obstacle (34%), reflecting concerns by service firms (37%) and manufacturers (35%).[11] Anecdotally businesses have also raised that the younger generations tend to be less resilient.

Recruitment and retention are major issues for businesses, including for colleges and other providers needed to train the next generation and upskill the current workforce. Employers have future and current employees wanting to train and upskill, but firms' cost bases – particularly post-Autumn Budget – have reduced their readiness to invest in futureproofing.

The CBI is calling for immediate reform of the Apprenticeship Levy, in anticipation of a more flexible Growth and Skills Levy next year, to allow firms to spend their funds on any training that is part of regulated qualification or accredited training course – as well as apprenticeships. A CBI survey[12] found that, under this policy change, levy-payers would invest an additional 30% of their levy over the next 12 months for training.

And with the ability to invest levy funds into short courses in digital and green skills, like cyber and robotics, retrofitting and heat-pump installation, employers will become more resilient and ready to create sustainable growth opportunities – both now and in the future.

Access to finance

According to CBI surveys, access to finance is a main concern for 29% of the respondents. This is against a backdrop of tight cashflow for many businesses facing extremely high cost bases, and therefore constrained spending and investment decisions, focused on the short-, not the long-term.

Some members highlighted the complexity and time-consuming nature of the UK business funding system as compared to similar schemes put in in place by international competitors such as the US and European countries. High thresholds and lengthy processes contribute to making access to cash more difficult for companies and consequently more complicated to invest in resilience building measures. When considering access to finance, this should include all businesses, including sole trader and partnerships to ensure all business models are captured.

To streamline access to finance, it is important to consider where there is a role for government incentives, but to also involve industry early in discussions with the government. This approach will help companies understand where they might need additional support.

SMEs face significant challenges in understanding and applying for funding due to insufficient information. Revising procurement rules could help to better integrate SMEs and address inconsistencies, thereby enabling more effective business strategy planning. SMEs also consider resilience related to surplus capacity, and the ability of stockpiling and moving resources. The way in which small businesses can access (or not access) finance and the cost of capital and cash to hold surplus capacity or stock are all obstacles to resilience.

The unpredictability of global events, particularly since the 2020 pandemic, has highlighted the fragility of global commerce and spurred a change in mindset for businesses reliant on international supply chains. Many companies have opted to on-shore or near-shore production and sourcing to reduce their supply chains' vulnerability to global disruptions. Others have increased inventory levels to better prepare for potential disruptions. A key aspect of this resilience is ensuring the availability of access to cash. Having sufficient working capital allows companies to maintain smooth operations even during disruptions and enables firms to quickly address unexpected challenges, such as sudden increases in supply costs or delays, without compromising their financial stability. This liquidity is essential for securing alternative suppliers, expediting shipments, and investing in technologies that enhance supply chain visibility and efficiency. By prioritising working capital management, businesses can better withstand economic shocks and maintain continuity, fostering a more resilient and adaptable supply chain.

Difficulties assessing risk

The context in which business operates has changed dramatically. Taking cybersecurity, for example, a recent publication by Cisco shows that 73% of the companies surveyed believe that a cybersecurity incident will disrupt their business in the next 12-24 months.[13] Lack of risk assessment and delays in information sharing cause significant operational challenges to businesses, and this is heightened for SMEs. These businesses face a higher likelihood that any risks they encounter will be existential in nature compared to large companies. About 24% of businesses reported difficulty of assessing risks as the main obstacle for investing in resilience.[14]

The government risk register has been cited as a useful tool to identify risks, but businesses would like to see the next level of detail down that can help them understand how to mitigate those risks identified. This becomes even more important for those risks that have greater unknowns such as cyber. While business welcomed existing measures and government initiatives such as the Cybersecurity and Infrastructure Security Agency (CISA) in the US and the National Cyber Security Centre (NCSC) in the UK, they feel government can go further to provide updated government guidance, particularly for SMEs. Timely information sharing i.e. on trade deals on sanction is a key component of business resilience, including for SMEs. Industry recognises that confidentiality bounds many of the critical information that should be exchanged and commits to find actionable solutions with the government on this.

The current evolving landscape necessitates more comprehensive and accessible resources to help businesses mitigate risks. Furthermore, there are several ways businesses could learn from each other in forums facilitated by the government:

- By undertaking testing collectively across sectors for scale and efficiency,
- Sharing best practice across sectors would help to upskill some businesses (e.g. manufacturers) that are newer to facing certain risks such as geopolitical risk than others (e.g. aerospace).
- Large corporates sharing scenario planning and mitigation strategies with their supply chains who are typically smaller in size and do not have the in-house capabilities.

The Cabinet Office's development of a Resilience Academy is a positive start, aiming to equip businesses with the necessary tools and knowledge to enhance their resilience through training modules, best practice frameworks and practical support.

Recommendation 6: The government's review of national resilience alongside the Industrial Strategy should identify where market failures exist in the uptake of resilience-based investments, and where there are information asymmetries. This should involve the following:

- Build upon existing training solutions (apprenticeships, bootcamps, etc) to more flexible and modular options, utilising the Growth and Skills Levy to act as an incentive to employer investment in skills;
- Exploration of how the new Resilience Academy can act as a forum for information sharing across sectors;
- Examination of whether there is a market failure in accessing finance for resilience purposes and where the funding system could support firms to both build resilience and to access the cash needed to cope with shocks as and when they arise. The CBI stands ready to investigate this further to ensure all businesses are able to access the finance they need to build their operational resilience;
- Through the resilience review, continue to work with stakeholders to establish a consolidated mechanism for timely information sharing with businesses about upcoming risks and potential consequences. The CBI stands ready to work more closely with government on ensuring the most effective mechanisms for information sharing with business in both directions.

Reference

1 Including the Resilience Framework, the Integrated Review, the Critical Imports and Supply Chains Strategy, the Semiconductor Strategy, the Cyber Security Strategy, and the Critical Minerals Strategy.

2 **Covid-19 Inquiry Module One: Oral Statement** 19 July 2024

3 Aggregation of data from different CBI surveys of June 2024

4 **No weak links: building supply chain resilience report.**

5 **WEF_Building_a_Resilient_Tomorrow_2024.pdf (weforum.org)**

6 **Oxford Economics Global Scenarios, June 2024**

7 Aggregation of data from different CBI surveys of June 2024

8 Aggregation of data from different CBI surveys of June 2024

9 Aggregation of data from different CBI surveys of June 2024

10 Aggregation of data from different CBI surveys of June 2024

11 Aggregation of data from different CBI survey of June 2024

12 **CBI education and skill survey 2022**

13 **Cisco Cybersecurity Readiness Index 2024**

14 Aggregation of data from different CBI surveys of June 2024

November 2024

cbi.org.uk