TRAVELERS

Rebuilding confidence

Managing mid-market risk to catalyse growth

Contents

Finding the confidence to grow

Mid-market businesses across the UK and Ireland are navigating a period of sustained external pressure. Our survey of 200 C-suite leaders and risk managers shows a clear picture: they remain confident in their own prospects, but are cautious about investing in growth against a backdrop of economic, geopolitical and regulatory change.

This report examines the factors shaping that tension. It highlights the external risks businesses feel least able to control, alongside the internal challenges that may be holding back investment and decision-making.

For brokers, this creates an opportunity. Understanding how clients perceive risk, and where their concerns are most acute, allows for more informed and relevant conversations.

The findings combine quantitative data with direct commentary from business leaders to offer a practical view of where attention is focused today.

Key themes include cyber risk, supply chain disruption, management liability and the evolving implications of AI. Across these areas, one message is consistent: businesses want to move forward, but need greater certainty to do so.

Brokers can support clients in focusing on what they can control, while remaining resilient to what they cannot

Insurance cannot remove every source of pressure. It can, however, help businesses manage exposures that might otherwise distract from growth. By addressing these areas, brokers can support clients in focusing on what they can control, while remaining resilient to what they cannot.

This report is intended to support those conversations, providing insight that helps brokers strengthen client relationships and respond to the challenges shaping the mid-market today.

This isn't about selling cover. It's about unleashing confidence.

Self-confidence is not enough

Mid-market ambition is strong – and can be unleashed if we help simplify a complex matrix of risks.

Mid-market businesses in the UK and Ireland contribute around £1.5trn (€1.7trn) in annual revenues and employ nearly eight million people.[1] But a cocktail of risks blight companies' confidence, stifling their instincts to take the risks that could drive growth.

Geopolitics, taxation, regulations, inflation, capital costs and demand instability all loom large in mid-market execs' thinking.

It's tough, they told us, to plan in an environment where consumer confidence, fiscal policy and operating costs move more than forecast models can absorb.

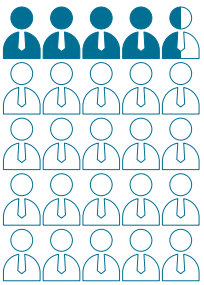
It's this increased volatility and risk, rather than a lack of ambition, that's holding them back.

Our survey revealed:

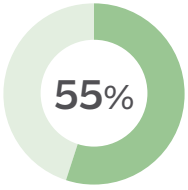
On risk...

88% say the risk environment is static or getting worse. The economy and their own profitability were key drivers, but staffing, skills, regulations and technology risks were all key.

88%
of executives think the risk environment is static or getting worse



Only 18% are less confident in their own business



feel only "somewhat resilient" to shocks

On confidence...

36% of respondents told us their confidence in the economy is falling. But only 18% are less confident in their own business, highlighting a disconnect between external uncertainty and internal ambition.

Helping them pick off the risks that inhibit investment will allow them to turn self-confidence into growth.

On resilience...

Business leaders told us they face a host of disruptions, any one of which could threaten their viability.

A worrying 55% said they were only "somewhat resilient" to shocks – driving understandable caution about change. Nearly half said they felt vulnerable to tech outages.

On cyber...

39% of execs said they'd faced a significant disruption over the past year due to cyber-related IT failures. Technology investment is a compelling option for growth, but they need confidence to deploy it.

Mid-market desire to invest and grow remains strong. Taking key risks off boardroom agendas could make decisions feel more doable

On AI...

More than half of mid-market firms think there are considerable data security and privacy risks with this transformative technology; only 12% said it poses no major risks. But many mid-market leaders said they felt it was inevitable. How will they square the competitive edge with new risks?

We can help unlock their confidence by simplifying this increasingly complex matrix of risks: removing the ones we can mitigate, equipping businesses with fresh options and allowing mid-market decision-makers to focus their efforts on navigating a volatile economic landscape.

The data reveals three major opportunity areas for brokers:

1. Revenue protection. Firms feel most exposed to demand shocks, unstable supply chains and geopolitical risk. Any approach that smooths future earnings – whether it's loss prevention or diversification – will boost confidence.

2. Capital efficiency. Faced with high debt costs and low risk appetite, products such as structured credit and business interruption cover reduce the need to hold capital against risk, freeing up cash to invest.

3. Technology transformation. AI, and digitalisation more broadly, can deliver automation and insight, addressing some prevalent risks. But execs worry about cyber exposure, model failure and systems resilience.

The mid-market desire to invest and grow remains strong. But to press forward without mitigating the risks feels foolhardy. The right cover, taking key risks off boardroom agendas, could make those decisions rational again.

Read on to find out more about attitudes to risk and confidence, and how cover could lift the burden.

Methodology

Our survey targeted mid-market UK & Ireland companies (revenue from €/£20m to €/£500m, between 50 and 500 employees) for this report. YouGov was commissioned to run a quantitative and qualitative survey between December 2025 and January 2026. The sample was drawn from a number of sectors, with additional research conducted across target sector companies.

Unpick the risk matrix

Complex, interrelated and unpredictable risks compel mid-market businesses to tread cautiously – 88% think the risk environment is static or worsening. Deal with risks that can be managed, and you create space to plan for those that can't.

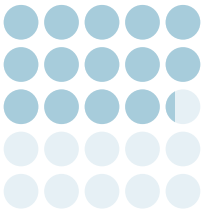
Today, every decision management makes can feel critical. It's partly the unpredictability of the risk landscape that poses the biggest challenge: economic shocks, policy shifts, technological disruption and geopolitical tensions are interacting in ways that make planning more difficult than ever before. Add in skills shortages, tech disruption and networked supply chains, and the mission is daunting.

We wanted to understand how these risks are coming together as a matrix – and identify which are most in need of mitigation for UK and Irish company leaders. With just 10% of our respondents saying that overall risk had reduced over the previous quarter, this need to unpick the risk landscape feels timely.

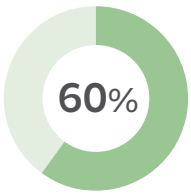
Risks on the ground

We asked mid-market leaders to identify the risks that most affect day-to-day operations (see fig. 1). A majority (60%) cited the economy. Cyberattacks – the highest-ranking risk factor we can insure against – and profitability were both mentioned by 47% of respondents, with AI and new technology not far behind, at 42%.

Analysis of the comments from our survey reveals that a big challenge right now is volatility: policy decisions, the economy and technological threats are shifting faster than they can adapt. (We conducted the survey before recent oil and gas shocks, for example.)



57%
consider the insurance market to be good at helping them manage risk



identify the economy as a critical risk factor

Against that backdrop, even growth itself becomes a risk decision. Businesses need to feel that investment decisions – a new warehouse, say, or rolling out a cloud-based SaaS platform – aren't injecting additional risks into that matrix. That means isolating and transferring specific exposures. That's why insurance – and brokers who can structure it effectively – can play a critical role in opening up growth opportunities.

Then we asked about risks affecting longer-term strategic decisions (see fig. 2). The concerns were all very familiar – profitability and the economy were joined by skills and recruitment, with cybersecurity still highly ranked. Mid-market execs believe these risks will persist – which creates a demand for long-term solutions. Take concerns about trading with overseas partners, rolling out new technology, or investing in skills development off their plate, and they'll have more freedom to tackle these fundamental barriers to growth.

The three risk clusters

Most of the pressures facing mid-market firms fall into three clusters:

1. Macroeconomic and policy volatility

Planning horizons are shrinking, forcing more reactive decision-making. Inflation, margin compression, weak demand and unstable

Figure 1
Which of these risks have been top of mind for you lately regarding day-to-day operations?

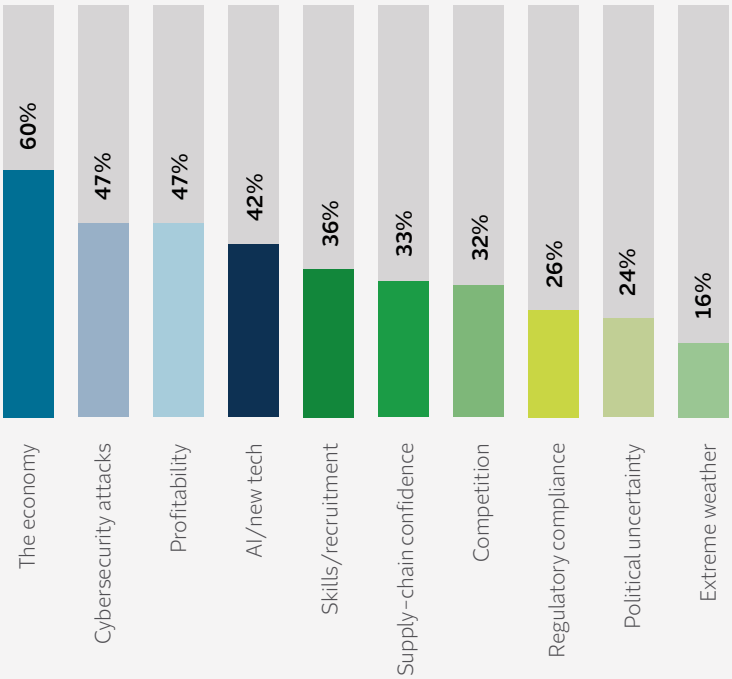
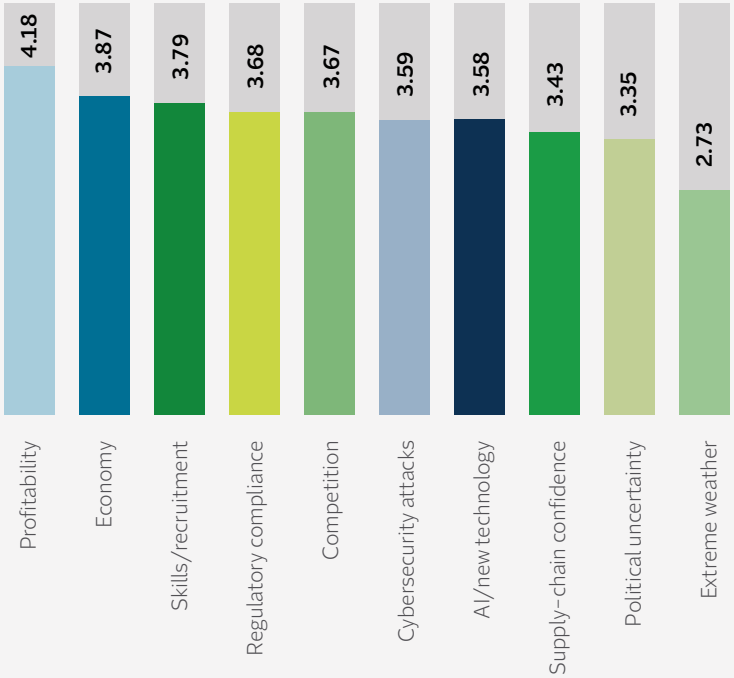


Figure 2
Which of these risks are most affecting your long-term strategy? (Average, scored out of five)



policy signals are making capital allocation harder. One respondent simply cited "economic uncertainty" as the core problem.

Add geopolitical volatility to the mix – which negatively affects markets and supply chains, and has a huge influence on all investment decisions right now – and you have a recipe for business inertia. Although these risks cannot be insured directly, by helping businesses to transfer exposures that *are* insurable, brokers can free up risk capacity for firms to move forward amid wider macroeconomic uncertainty.

2. Technology and cyber disruption

Cybersecurity concerns, rapid tech evolution and whole-business digitalisation are creating a single catastrophic point of failure. That means risk mitigation, on cyber particularly, can give boards a direct confidence boost. While the nature of cyber threats – and the types of cover available – has developed, company policy sometimes has not. With technology a key enabler of efficiency, this is a huge opportunity.

According to UK Government data, mid-market firms are far more likely to rely on cybersecurity cover embedded within wider insurance policies (47%) than on dedicated cyber policies (18%).[2] One in five businesses said they did not know whether they had any form of cyber insurance at all. This represents a clear opportunity.

3. Workforce and supply chain

Skills shortages and supply-chain fragility are now viewed not as operational challenges, but as strategic risks to growth. The mid-market relies on contractual relationships – with employees, suppliers and customers.

These pressures are amplified by wider regulatory developments. "It's the risk of taking on new staff in the UK (due to proposed changes in employment laws) versus investing in hiring new staff in other countries where employment legislation is less onerous," said one respondent. Irish firms are less troubled by regulation (although it's still a top-three risk, according to

local research by Grant Thornton[3]), but 54% still see skills shortages as a barrier to growth.

Retaining high-value employees is therefore critical. Insurance can play a direct role in this, with employee benefits and wellbeing programmes supporting engagement and long-term loyalty. At a senior level, comprehensive directors & officers liability cover can give executives the confidence to make bolder decisions around investment and growth, knowing they are protected. Alongside this, policies such as business interruption and trade credit insurance help businesses manage supply chain disruption and operational shocks, reducing uncertainty for both leadership teams and the wider workforce.

Shifting mindsets

Mid-market companies know how to grow. What many struggle with is justifying the downside exposure of investing in an era of "permavolatility". To pursue opportunity, they need to manage the risks they can control – and build resilience against those they cannot.

More than half of all respondents (57%) believe the insurance market is good or very good at helping them manage risk. Within that group, 56% feel "very resilient" around

To pursue opportunity, mid-market businesses need to manage the risks they can control – and build resilience against those they cannot

risk, compared to just 26% of those who were neutral about insurance, and 14% of those whose attitude was negative. Correlation is not causation; but that suggests the right cover can play a role in building resilience.

The message is clear: brokers who help businesses navigate risk effectively become strategic partners.

Those who can help clients de-risk – be it in transformation, international expansion, technology adoption, workforce strategy or capital investment – are more than providers of cover. They become providers of risk capacity, helping organisations evolve with confidence.

And when that happens, cover stops being seen as a cost. That's when insurance becomes a strategic enabler of growth and resilience.

Summary

- Volatility is the key challenge. Unpredictable economic and geopolitical conditions shorten planning horizons and temper decision-making.
- Mid-market risk falls into three clusters: macroeconomic and policy volatility, technology and cyber disruption, and workforce and supply-chain pressures.
- Brokers can help restore confidence. Mitigating insurable risks gives businesses more risk capacity for growth opportunities.

Closing the confidence gap

Confidence is the fuel of mid-market growth. But when economic signals are unclear, even ambitious businesses hesitate to commit capital.

Figure 3
The circle of confidence

Confidence in the mid-market is a feedback loop. When businesses feel positive about their own prospects, they invest, they hire and they expand. That helps drive wider economic growth – which, in turn, reinforces their confidence.

But that circle depends on one crucial ingredient: predictability. When the economic backdrop is volatile, the circle breaks down. Insurance can prove critical in isolating a range of risks, removing them from the equation. For example, businesses that are covered against business interruption are more likely to invest in new supply-chain relationships; knowing a cyber incident will be handled by a professional response team makes new tech feel less risky.

The confidence gap

Although there is a correlation between overall economic confidence and business confidence, execs tend to be more confident in their own business than in the wider economy (see fig. 4).

Overall, 36% of C-suite executives report being less confident in the wider economy, quarter-on-quarter. But just 18% say their confidence in

their own business has fallen. UK and Irish mid-market decision-makers believe in themselves – but they need their home economies to offer more hope if they are to grow.

"What we're seeing isn't a lack of ambition in the mid-market," says James Hampson, a portfolio manager at Travelers. "It's a hesitation to commit capital when the downside feels hard to control."

Reduce the number and severity of the downside risks, then, and confidence to invest rises.

Defensive pragmatism

Surveys by the British Chambers of Commerce[4] and the Confederation of British Industry[5] both confirm that gap between confidence in firms' own prospects and optimism about the national economy. In Ireland, according to Grant Thornton, net optimism among mid-market leaders fell from 81% to 54% during 2025, with expectations for profitability and hiring following a similar trend.[6]

The consensus is that mid-market companies can adapt to "permavolatility". They accept that economic conditions are challenging,

Mid-market companies can adapt to 'permavolatility', and still want to increase market share when the risk of doing so is clear and well-managed

and still want to increase market share via operational discipline when the risk of doing so is clear and well-managed. Across both markets, the prevailing mindset is best described as "defensive pragmatism": manage costs tightly, invest selectively and pursue growth cautiously.

"The thing that would make the biggest difference to us is a more predictable and supportive environment," said one survey respondent, "whether that's steadier customer demand, clearer market signals, or resources that let us plan with confidence and focus on growth rather than reacting to uncertainty."

Confidence in action

This is where we see a clear link between well-managed risk and business confidence. Get the cover right, boost the feeling of resilience to shocks, and confidence builds.

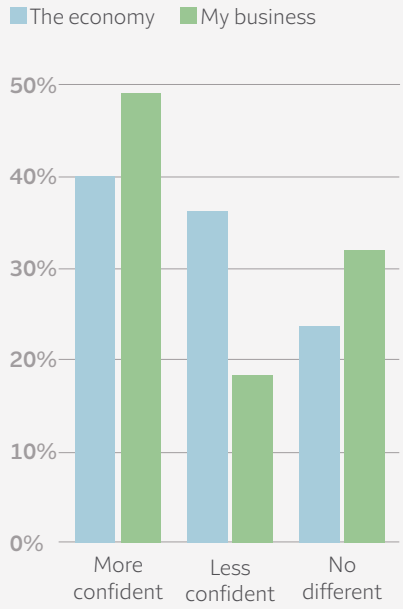
Take cyber. Among execs who say they are relaxed or confident about their cybersecurity arrangements, 70% report growing confidence in their business outlook (compared with 49% across all respondents). Among those *concerned* about cyber preparedness, only 20% report rising confidence.

In other words, when businesses feel they have control over key risks, they become more confident about their future – and more willing to invest – despite the unsettled economic backdrop. This places insurance squarely in the frame as a driver of wider business confidence.

Sector signals

How that confidence translates into action varies significantly between

Figure 4
The confidence gap: quarter-on-quarter change



sectors. But our survey responses, combined with wider business sentiment data, reveal several consistent patterns (see chart on page 11).

Resilience through agility

What all the risk mitigations we offer have in common is that they boost organisational resilience. And given the headline finding from our survey – that 96% of respondents believe their businesses are resilient – the broader picture seems optimistic.

But there's a nuance to that finding: a majority (55%) describe themselves as only "somewhat resilient" rather than "very resilient". And that distinction matters. It suggests many believe they can continue operating through disruption, but are less certain about how well they would withstand a major, unexpected shock.

Companies' appetite for cover reflects this. "We're seeing businesses become more willing to invest in higher limits and broader coverage as they recognise that single incidents can threaten business viability," says Ruth Reaney, head of Health and Care at Travelers.

As one respondent put it: "Economic instability, cybersecurity threats, talent shortages, supply-chain disruptions and emerging AI risks... these pressures make resilience and agility essential."

That need for agility explains why instilling confidence around digitalisation (and other developments that underpin rapid change in how businesses operate) is so important right now. Measures that protect cash flow, support employees and reduce exposure to operational shocks can all help strengthen resilience.

That's why business interruption, directors & officers liability cover, proactive rehabilitation in employee health policies and even the wellness components of cyber cover are so valuable to the mid-market. It's about getting systems and people up and running after a crisis. More importantly, perhaps, they also back up a flexible and open-minded approach within a rapidly changing business environment.

Today, cover is about creating a capacity to withstand disruption, freeing up management to plan ahead and take calculated risks.

Summary

- Business confidence remains stronger than economic confidence. Mid-market leaders generally believe their firms are resilient despite being cautious on the wider economy.
- Predictability drives confidence. Stability in demand, costs and regulation would allow firms to plan and invest more decisively.
- Managing risk strengthens confidence. Being better prepared for threats such as cyber disruption gives firms faith in their growth prospects.

Sector	Effect of confidence	Current situation	Insurance solutions
Manufacturing	Investment in innovation and export capacity, particularly where firms see opportunities in international markets	Hiring is subdued, reflecting ongoing cost discipline and geopolitical uncertainty	✓ Leverage balance sheet: deploy capital otherwise held against losses to other risk factors ✓ Surety for international contracts ✓ Trade credit protection
Services	Productivity investment, particularly automation and digital tools	Some sub-sectors are reducing headcount even as confidence improves, with technology and outsourcing reshaping operating models	✓ Employers' liability – protection against injury and absence ✓ Proactive rehabilitation services minimise staff disruption ✓ Cyber policies to boost confidence in digital transformation ✓ Disaster recovery guarantee to get back up and running in 24hrs
Retail	Defensive optimisation rather than expansion	Firms focused on supply-chain resilience, cost control and adaptability to shifting consumer behaviour, rather than long-term commitments	✓ Specialist business interruption ✓ Specialist property damage, including glass and lettering ✓ Cyber cover designed for e-commerce

From cyber risk to investment confidence

Mid-market businesses are attractive to hackers – a worthwhile target, but often without dedicated cyber defences. This represents an opportunity to inject confidence via cover.

We've looked at the complex risk matrix that hampers UK and Irish mid-market growth. And we've seen how C-suite confidence and resilience are boosted when the risks are addressed. What does that look like in practice?

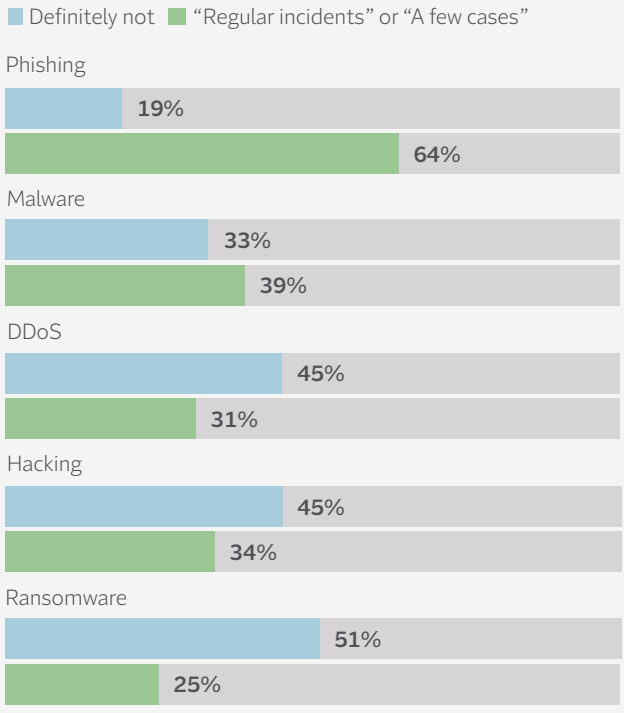
Cybersecurity – one of the biggest risks cited in our survey – is a perfect example of how we can help the mid-market grow in the face of unpredictability. Nearly half of mid-market leaders told us they are either "relaxed" or "confident" about their business's cybersecurity arrangements. But is that confidence misplaced?

"Cybersecurity complacency could be one of the largest risks a mid-market business faces," says Jon Preston, practice lead for Technology at Travelers. "That's especially true as bad actors become more effective and start using AI to enhance their attack methods."

At a time when digitalisation is a key engine to increase efficiency, boost agility, and open new avenues for growth, cyber becomes a central node in the risk matrix. If we can help mid-market businesses gain confidence that these acute and novel risks to new technology can be managed, we drive up confidence and help address a host of other risks in that matrix, too – from supply chain resilience to directors' liability.

Across most categories of cyber threat, only around half of respondents could say with certainty that their business had *not* been targeted by an attack. Nearly two-thirds report regular phishing attempts, while a quarter have been targeted by ransomware (see fig. 5). Overall, 39% of mid-market C-suite executives in our survey report "significant disruption" over the past year linked to cyber-related IT failures.

Figure 5
Under attack: "Which of the following cyber threats have you had to deal with and how frequently?"



These findings align with wider research. The UK Cyber Security Breaches Survey 2025[7] found that 43% of businesses identified a cyber breach or attack in the past 12 months, while 20% were victims of at least one cyber crime.

Among mid-market firms, the incidence of cyber crime is *twice* the overall business average. That's prompting a fresh look at mitigation efforts (including insurance). In Ireland, according to PwC's Global Digital Trust Insights, 57% of organisations are increasing investment in cyber risk management.[8]

"Protecting customer data and preventing breaches is becoming more challenging," said one respondent. If the C-suite fear digital transformation might introduce new risks or increase exposure in the event of an attack, it will inhibit crucial investment in that technology.

A growing risk for the mid-market

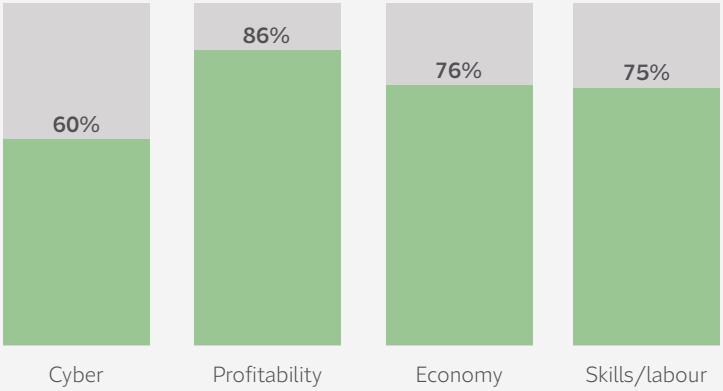
Large organisations typically maintain dedicated internal cyber teams and extensive training programmes. Mid-market firms, however, are large enough to attract sophisticated attacks yet often lack the scale to invest in deeply specialised cyber defences.

With the threat landscape changing so rapidly, mitigation needs to evolve too. In Ireland, for example, Expleo figures[9] reveal that 41% of mid-market organisations experienced an *AI-powered* cyberattack in the past year. "If business leaders aren't aware of how threats are developing, especially with AI, they may not focus the required resources on it," Preston says.

The growing risk is also triggering a regulatory response. Figures from the National Cyber Security Centre (NCSC)[10] reveal that the number of "nationally significant" incidents more than doubled last year; the most serious category of attacks increased by 50%. Legislation to enforce the cyber resilience of nationally significant infrastructure is now before the UK Parliament.

High-profile incidents affecting Jaguar Land Rover, M&S and the Co-op showed how quickly chaos can spread through connected systems and supply chains. Businesses may suffer major disruption without even being targeted – and yet just 14% of UK businesses have reviewed the cyber risk of their immediate suppliers in the past 12 months, according to Government data.[11]

Figure 6
What features regularly on your board agenda?



Bridging the knowledge gap

Worryingly, while 60% of respondents told us cyber is regularly on their board agenda (see fig. 6), that's well behind issues such as profitability, skills shortages and the economy. Yet the implications of a cyberattack extend far beyond IT systems. "Cyber insurance isn't just about covering the financial losses from an attack," Preston explains. "It's also about understanding the entry route, ensuring the attack is completely removed and providing recommendations that make future attacks less likely."

In addition to financial protection, cyber policies can provide specialist response support and technical expertise during incidents. "Travelers offers proactive cyber risk mitigation advice from in-house IT experts," Preston adds. "We can help clients avoid the major disruption a cyberattack – even an unsuccessful one – can cause."

A leadership issue

Cyber illustrates how the risk matrix works. It's not just the risk of your systems going down;

there's data protection, supply chain, and regulatory compliance to consider, as well as potentially significant governance and liability questions for the board. "Directors need to think about whether a claim could be brought against them following a cyberattack if the company didn't purchase cyber cover – or didn't purchase enough," says Geoff Hick, head of private D&O at Travelers. "They may also face regulatory scrutiny, including potential claims from bodies such as the Information Commissioner's Office."

On top of that, cyber breaches are not only technological events – they can have a profound human impact, placing employees under intense stress. Effective cyber cover, therefore, extends beyond IT systems. It requires leadership awareness, clear governance and well-rehearsed incident response plans that support both the organisation and its people once the dust has settled.

Summary

- Cyber risk is a leadership issue. Boards need a clear understanding of how cyber threats evolve and how prepared the organisation is to respond. Good cover should include readiness audits, breach planning and system restoration pathways.
- Education is critical. Executives who understand how cyberattacks develop, particularly with the growing use of AI, are far better positioned to allocate resources effectively. Brokers who can advise on this are well-placed to be seen as strategic partners.
- Preparation matters as much as prevention. Cyber insurance and specialist incident response support can help organisations contain attacks, recover quickly and strengthen their resilience against future incidents – not just remediate losses.

AI: a new risk vector

Our survey suggests that just over 40% of mid-market firms have already deployed some form of AI technology. Given how recent the technology's emergence is, adoption has been remarkably swift. And its strategic importance has embedded rapidly, with 54% of executives telling us that AI will be either "significant" or "key" to their future strategy.

Respondents frequently cited AI, automation and data capabilities as key drivers of future productivity and growth. Digital transformation has the potential to help mid-market leaders address a host of issues within the volatile risk matrix we've been discussing. But without adequate mitigation of the new risks they introduce with AI, this investment can be nerve-wracking.

"The potential for being compromised via AI is extensive," says James Doswell, senior risk management consultant at Travelers. "There is a dual risk: being targeted by AI-powered attacks, but also having your own legitimate AI products exploited as an attack vector. We've seen experiments using autonomous agentic AI systems with swarm capabilities that compromise environments incredibly quickly."

Cyber cover can make a difference here, but a considered and holistic approach is needed.

Understand the security implications
AI systems can introduce new vulnerabilities, from data leakage to AI-enabled cyberattacks. Review cyber readiness and update policies in light of new attack vectors.

Strengthen governance and oversight
Boards need clear policies covering AI use, vendor relationships and regulatory compliance. Assess liability cover around key digitalisation decisions.

Focus on value as well as innovation
AI investment must deliver measurable productivity or growth benefits. Assess overall risk appetite in light of opportunities.

Different sectors, different concerns

In the previous chapters we looked at the macro factors affecting the mid-market. Here, we look at how sentiment, challenges and solutions differ across three industries: tech, health and care, and manufacturing.

Technology: Confidence in a high-risk environment

Tech execs are much more confident than those in other sectors: three-quarters of them report rising confidence in their own organisations, compared with a mere third of non-tech businesses.

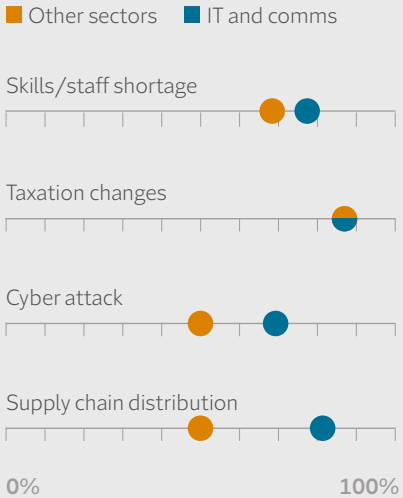
The reason for this? Demand. Digital transformation, cybersecurity spending and the rapid emergence of AI continue to drive demand for many technology services. Even when clients delay projects in uncertain economic conditions, they rarely abandon core technology investments altogether.

This need to stay abreast of tech developments is doubly important for tech businesses themselves. "AI changes are pretty huge and we know we need to be AI-first," says Rupert Bedell, managing director at Gloucester-based internet provider Fasthosts. "On top of rapid growth for our core services, it's a big challenge."

Risk at the heart of the sector

But the same forces driving this demand create significant risk exposure. Software vendors, cloud providers, outsourcing specialists and IT consultancies are all prime targets for cyberattack because they

Figure 7: technology
Significant disruptors



often hold sensitive data or provide access to client systems.

This makes robust security an essential competitive differentiator for tech firms. “Cybersecurity is no longer just a cost centre,” said one respondent. “It’s a selling point. Our strong security posture is helping us win contracts with larger enterprise clients.”

Supply chains and skills

Cyber risk is not the sector’s only structural challenge. Many mid-market technology firms rely on a relatively small group of upstream providers, including hyperscale cloud platforms and major software vendors. That concentration introduces supply chain risk, where any outages or disruptions can quickly cascade through to customers and partners.

Skills shortages are a persistent and growing concern too. UK government research shows that 28% of cyber-sector businesses report critical technical skills gaps[12] (up from 18% in 2021). And analysis from Trinity Business School indicates Ireland’s cyber sector is overdependent on international talent.[13]

Tech concerns

- Tech leaders’ confidence in their business far outstrips the average.
- Risk exposure, particularly from cyber threats and dependence on cloud and SaaS providers, is significant.
- Skills shortages constrain resilience.
- Rapid incident response and recovery capability increasingly define resilience.

Building resilience

For many firms, resilience depends on how quickly they can respond to disruption, rather than whether disruption occurs at all. “We can’t block every risk, so we are focusing on rapid detection and response,” said one respondent. Companies will fall prey to hacks, then, but it’s how they respond that matters. “Our ability to recover quickly from incidents gives us a distinct advantage,” said a second respondent.

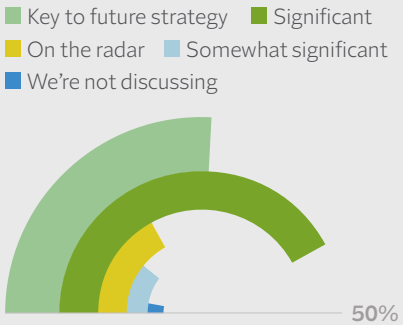
Policies that support rapid recovery after cyber incidents can therefore play an important role – not only by protecting operations in the event of an attack, but by reassuring employees and clients that risks are being managed effectively. “Risk management is more connected to business and people outcomes than it is often treated,” says Chris Scott, director of Claim Management at Travelers.

In a sector defined by rapid change, minimising cyber-related disruption – to insure a business and its people recover quickly – can be every bit as important as innovation.

Health and care: Demand outweighs capacity

Ageing populations, rising healthcare needs and growing interest in private provision keep health and care leaders confident regarding long-term demand for their services. But that confidence is tempered by the sector’s ability to deliver its services.

Figure 8: health and care
How important is staffing to your business?



Funding pressures, workforce shortages and regulatory constraints suppress positivity; despite a small jump, from −21 to −16, Lloyds Bank's Healthcare Confidence Index remains negative.[14]

Survey respondent Mark Smith, director of PMI at Nuffield Health, summed up both head- and tailwinds. "There's optimism around the impact of tech solutions – not just clinically, but to support efficiency and manage costs – but there are long-standing issues around staff availability and newer concerns about rising employment costs."

A workforce under strain

Workforce challenges remain the sector's most persistent constraint. Skills for Care estimates 111,000 vacancies across the UK care sector, with staff turnover running at roughly 25%.[15] International recruitment – which previously helped ease shortages – has declined sharply, halving from a recent high of 105,000.

Similar pressures exist in Ireland, where research by BDO and Nursing Homes Ireland highlights growing skills shortages, compounded by tighter regulatory controls on non-EEA migrant workers.[16] In our survey, respondents across all sectors ranked staffing and skills among their most important strategic priorities, second only to profitability and the economy.

Although the state-funded homecare sector grew by 11% last year, that may not be sustainable. "We are concerned that some homecare providers have said they are handing back local authority contracts due to rising costs," the Care Quality Commission warned in October.[17]

The challenge, then, is about operational resilience – maintaining services while navigating tight margins and staffing constraints.

Strengthening resilience

Policy clarity could help improve planning certainty, according to one respondent: "The biggest boost would be the Health Secretary bringing forward a clear plan to tackle the UK's healthcare priorities and then delivering it, so the private sector can plan alongside it."

Insurance may not be able to solve staffing shortages, funding pressures, or policy shortcomings, but it can stop operational shocks turning into existential threats. Liability cover and professional indemnity are essential protections in a sector where patient claims represent a significant risk. And employers' liability policies with rehabilitation and wellness support can also contribute to workforce retention and employee wellbeing.

"Wellness is a material factor across all sectors now – not a nice to have," says Alison Manley, director of customer relationship management at Travelers. "Services that support employees and foster loyalty can help address staffing issues, especially when you're competing for talent."

Supporting digital transformation

Heavy investment in digital technologies, to improve efficiency and patient care, creates its own risks. But operations can be protected via cyber resilience, incident response support and business interruption cover – allied with robust property insurance for premises-based services such as clinics and care homes.

Health and care concerns

- Demographic trends and growing private provision support demand.
- Workforce shortages blight both operational capacity and long-term planning.
- Financial pressures in state-funded care models test resilience.
- Effective risk management can help protect operations.

Manufacturing: Confidence under pressure

Across the mid-market as a whole, execs have more confidence in their own businesses than they do the wider economy. But for manufacturing the picture is bleaker: 40% of manufacturing leaders in our survey are less confident in their own

business prospects than they were three months ago – versus 18% of all respondents.

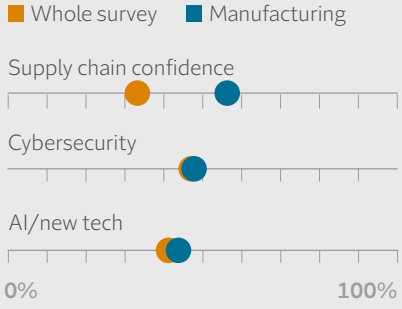
An above-average amount of manufacturers are also losing confidence in the economic outlook. This reflects the sector's exposure to global uncertainty; manufacturing businesses typically have complex supply chains, high capital investment and tight production schedules, making disruptions particularly costly.

"For many manufacturers, the question isn't 'Can we grow?' – it's 'Can we absorb the shock if something goes wrong while we're growing?'" says James Hampson, portfolio manager at Travelers. "Businesses need to ring-fence the consequences of disruption to have more confidence to invest."

The cost of disruption

For manufacturers, resilience often comes down to practical operational questions, says Richard Harrison, head of risk control at Travelers: "How quickly can specialist equipment be replaced? How dependent are you on a single supplier? And how prepared are you for an unplanned shutdown?"

Figure 9: manufacturing
What are your key concerns?



These are the kinds of risks that can halt production and quickly erode margins, with opaque supply chains a particular concern. As one respondent noted: "Supply chain transparency is improving, but we still struggle with visibility into Tier 2 suppliers."

Risk management and resilience

Many of the risks troubling manufacturers are, at least in part, insurable. Trade credit insurance, for example, can protect receivables and support financing when working capital is stretched. Business interruption cover and cyber insurance can help organisations recover more quickly when operations are disrupted.

Yet the benefits of these protections may not always be fully recognised. Only 28% of manufacturers said the insurance market had been good at helping them manage business risks (versus a survey average of 57%). Clearly, there's a gap between the risks manufacturers face and their perception of how effectively those risks can be managed.

This, in turn, presents an opportunity: to pick apart the risks they're facing and demonstrate how mitigating them – not just with cover, but with advice on management – could boost confidence.

Skills and automation

Lack of skilled staff in the manufacturing sector hampers its evolution. "We struggle to find qualified technicians to operate new automated systems," said one respondent.

Although skills shortages are primarily labour market or education challenges, organisations can still take steps to reduce their operational impact. Policies that support employee wellbeing, rehabilitation and workplace safety, for example, can help retain experienced staff. That's an important consideration for manufacturers competing for a limited pool of specialist technical talent.

Together, these measures can help organisations restrict the operational consequences of disruption, so leadership teams are more confident pursuing investment and growth.

Manufacturing concerns

- Manufacturers are low on confidence, reflecting exposure to operational and economic shocks.
- Supply chain complexity and cyber risk remain key concerns.
- Skills shortages slow adoption of automation and advanced manufacturing technologies.
- Better risk management can help ringfence disruption.

Turn complexity into confidence

Mid-market companies aren't lacking ambition, they're hamstrung by risk. Brokers can help them look beyond the obstacles, overcome fear and pursue growth

Our survey suggests that a combination of risks, complexity and uncertainty are the overriding concerns of the mid-market.

Historically, commercial insurance has positioned itself as a compensator, or even as a compliance requirement. But today's economy rewards those who can protect revenue, smooth volatility and unlock investment. The UK & Ireland mid-market doesn't need insurance because bad things might happen – it needs insurance because good things will *not* happen unless downside risk is controlled.

Mid-market firms aren't short on vision; they're short on risk capacity. Brokers are uniquely positioned to close that gap and those who help make that happen will be seen as strategic enablers – of capital deployment, transformation and resilience.

Where a client might be tempted to retrench in the face of uncertainty, offering to help that client invest and grow safely should speak more directly to mid-market execs' concerns. Travelers is ready to be a trusted partner on that journey.

In this final section of our report, we draw on direct quotes from our research to show how mid-market concerns have evolved – and suggest real-world advice for brokers to help them overcome those fears.

Risk	Typical concern	Mid-market request	Solutions
Tax and regulation	"I would like to see management liability mentioned under tax and regulation, as our policy protects both the directors and entity"	Can we make this a more predictable and supportive environment – where we're not caught out by non-compliance?	✓ Advisory on required protections ✓ Professional indemnity solutions reassure when regulations change rapidly
Business resilience	"Establishing stronger operational discipline, aligning our teams around clear priorities and driving consistent execution"	Reassure us that if something comes out of leftfield, it's not going to derail our hard work and investment	✓ Thoughtful property protections ✓ Trusted risk management advice ✓ Risk management funding ✓ Business resilience and continuity planning ✓ Health & safety management as a business enabler
Cybersecurity	"Protecting customer data and preventing breaches is becoming more challenging"	Give us the confidence to deploy new technologies and exploit connectivity when there are risks that we're still learning about	✓ Pre-cover review and proactive advice ✓ Rapid incident response ✓ Loss recovery ✓ System restoration and post-incident counselling
Margin compression	"Rising costs, particularly in energy and raw materials, are exerting pressure on our profit margins"	Find ways for us to free up capital and shift risk from the balance sheet to new opportunities	✓ Leverage balance sheet: deploy capital otherwise held against losses to risk factors ✓ Support diversification (new markets, new products)
Skills and talent shortages	"The shortage of skilled technicians in key sectors is hampering our capacity for development"	We need to protect and keep our people happy and productive, whatever the circumstances	✓ Employers' liability – protection against injury and absence ✓ Proactive rehabilitation services minimise disruption ✓ Health and safety-led risk engineering: prevention, not just claims
Geopolitics and trade	"Risks relating to global instability, economic uncertainties, FX instability and tariff wars"	Inject some confidence into our search for new markets by helping us address unfamiliar risks and uncertainties	✓ Trade credit protection ✓ Surety for international contracts
Supply chain resilience	"Supply chain disruptions have resulted in delays and increased costs for us"	Help us take on new customers and diversify suppliers to smooth costs and revenues – and guard against breakdowns	✓ Business Interruption (including contingent BI) addresses revenue volatility caused by downtime
AI and digital transformation	"The pace of tech change, AI regulations, and uncertainty about how AI impacts costs and workforce needs"	AI is evolving fast; to gain confidence we need help managing the risks and how it affects existing arenas	✓ Review of D&O and other liability policies ✓ Cyber insurance to guard against AI-powered attacks

TRAVELERS

Contact us

travelers.co.uk/contact-us
+44 (0)20 3207 6000

travelers.ie/contact-us
+353 (0)1 609 5600

References

1. Grant Thornton, Agents of Growth: The UK Mid-Market Report (London: Grant Thornton, 2023), which estimates that UK mid-market firms generate approximately £1.3 trillion in revenue and employ around 7.3 million people; Ireland adds approx. €100bn in turnover and 500k employees.

2. Department for Science, Innovation and Technology and Home Office, Cyber Security Breaches Survey 2024 (London: UK Government, 2024). The survey reports that 47% of medium-sized businesses (50–249 employees) have cyber risk covered within wider insurance policies, compared with 18% that hold a standalone cyber insurance policy, indicating a strong reliance on embedded cyber coverage among mid-sized firms.

3. Grant Thornton (2025). International Business Report (IBR): Ireland results, Q4 2025. Dublin: Grant Thornton Ireland. The survey of Irish mid-market businesses found 54% of respondents cited the availability of skilled workers as a constraint on growth.

4. British Chambers of Commerce, Quarterly Economic Survey (QES), various editions. The survey gathers responses from several thousand UK businesses each quarter and is one of the UK's largest independent indicators of business sentiment.

5. Confederation of British Industry (CBI), Economic Surveys and Business Optimism Index, various releases. The CBI surveys senior executives across UK industries to measure expectations for output, investment and the general business situation.

6. Grant Thornton, International Business Report, a quarterly survey of senior executives in mid-market businesses worldwide examining confidence, growth expectations and key business risks.

7. Cyber security breaches survey 2025. An annual official statistic detailing the frequency and impact of cyberattacks on businesses, charities and educational institutions.

8. PwC's Global Digital Trust Insights Survey 2025.

9. Expleo 2025 Business Transformation Index.

10. NCSC Annual Review 2025, the National Cyber Security Centre's ninth review of key developments and highlights, between 1 September 2024 and 31 August 2025.

11. NCSC, Cyber Essentials Supply Chain Playbook.

12. Cyber security skills in the UK labour market 2025.

13. Ireland's IT skills supply insufficient to meet future demand predictions.

14. Healthcare Confidence Index – Lloyds Bank Healthcare.

15. The State of the Adult Social Care Sector and Workforce in England.

16. Nursing Homes Ireland Annual Private Nursing Home Survey.

17. The State of Health Care and Adult Social Care in England.