beazley

Spotlight on Cyber Threats and Tech Advances 2026

Resilience in an AI-accelerated threat era

Executive summary

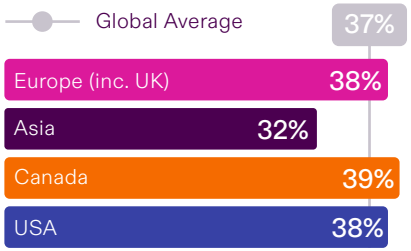
Cyber threats intensify. Tech advances. Resilience needs an urgent rethink

Systemic shifts are reshaping cyber risk

Cyber risk is the top concern for businesses worldwide, and with good reason. It's shifting into a different league. What was once seen as a tech issue, now represents a systemic, long-lasting threat capable of impacting every corner of an organisation and its supply chain.

Cyber criminals are now successfully using agentic AI to execute large-scale automated reconnaissance and phishing campaigns. These systems run elaborate attacks at speed and scale, exploiting the deeply interconnected and interdependent nature of today's technology ecosystems. This has created a threat landscape where attacks are faster, more adaptive and harder to detect or contain.

Cyber attack concern by region



Percentage of business leaders selecting cyber attack and the resultant system outage as a top three macro risk concern (2026/27 Risk & Resilience survey).

Multiple fronts, minimal warning

These dynamics create a perfect storm for organisations that are underprepared. Businesses of all sizes now face a tsunami of rapidly evolving threats coming from multiple sources simultaneously.

One example is cyber attacks driven by escalating global geopolitical tensions. Evidence already shows that Iran is targeting US companies and infrastructure with cyber retaliation attacks.

Global threats through an executive lens

These converging threats are harder to predict, govern and contain – and every new high-profile breach reinforces the speed of how the risk environment is intensifying.

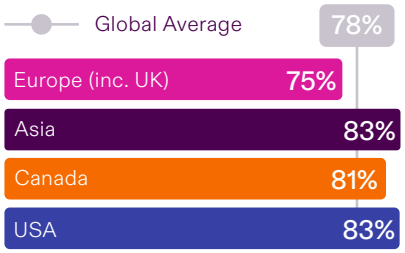
Since 2021, we have tracked global executive sentiment across key risk areas, giving a clear view of issues most likely to escalate across organisations, industries and regions. Read on to discover the cyber and technology risks executives find most concerning, their confidence in organisational resilience, and the preparedness gaps they see. This report outlines the actions needed to build stronger, more adaptive resilience for the challenges ahead.

Threats spread further and last longer

Just one small incident can unleash messy, expensive fallouts that could spiral into multi-line losses with the impact continuing long after the technical fix is done.

Yet **82%** of the global executives we surveyed say they feel 'prepared' for such risks; confidence that signals a critical underestimation of the dangers – breaches are now a matter of **when**, not **if**, and readiness will determine the outcome.

Cyber incident recovery confidence



Percentage of business leaders by region confident they could fully recover from the financial impact of a cyber attack (2026/27 Risk & Resilience survey).

Tech drives value, and vulnerability

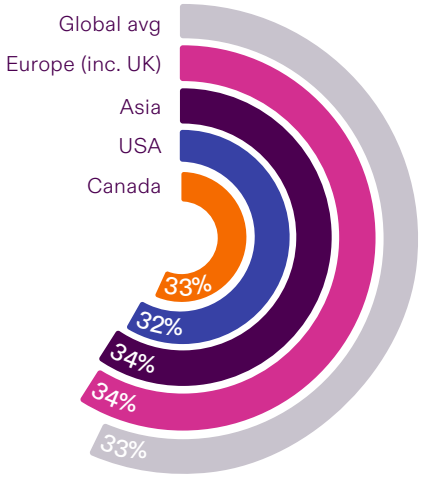
Technology is evolving at speed across industries, with agentic AI emerging as one of the most potent. The potential is compelling, but there are perils too, and firms need to grasp the full scope of these risks.

The upsides – speed, agility, efficiency – driven by automated decisions and data processing that provides richer data insights. These save time and resources while enabling the capacity to scale.

The dangers – these tools sit in attackers' hands too. Widening their attack surface and closing the distance between breach and damage.

AI-led tech disruption concern

Percentage of survey respondents by region that selected AI-led tech disruption, including bias, non-performance, system obsolescence and operational impact as a top three risk factor of concern.



Beazley 2026/27 Risk & Resilience survey.

Confronting the governance gap

AI acceleration is also exposing the gaps between rapid innovation and governance frameworks not designed for this pace of change. Insufficient oversight amplifies risk with ungoverned AI exposing sensitive data, while flawed AI decisions flow unchecked, fuelling privacy, compliance and operational consequences that grow faster than leaders can contain.

Cyber and technology risks need to be kept in check by system oversight, and firms must use the relevant tools available to help monitor, manage and warn of emerging threats, helping to stem them before they turn into something larger.

Rethinking resilience

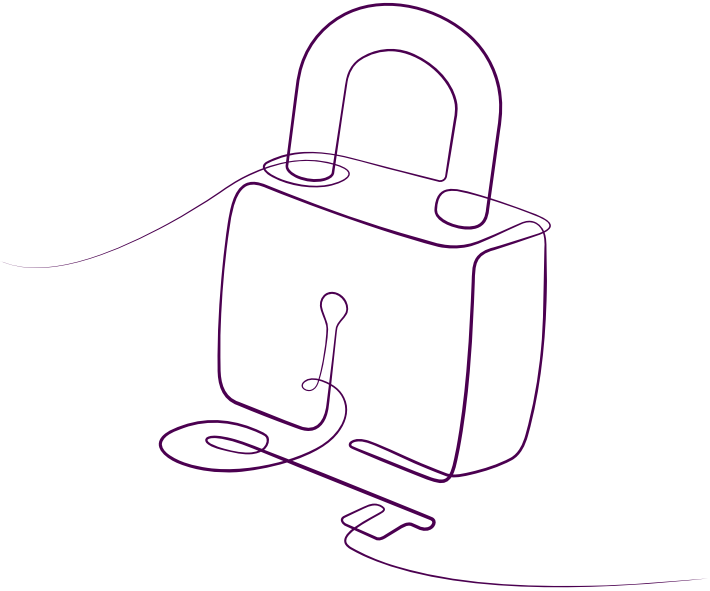
With business operations now predominantly digitally powered, business leaders must prioritise cyber resilience, as when a crisis hits, it's too late to build it.

Resilience should be embedded from the outset through well-planned and regularly tested business continuity plans that enable fast, efficient and effective response. Planning must also consider the true cost of an attack, including available financial capital to withstand the losses. This includes identifying insurance coverage levels, gaps in cover, and any blind spots in control mechanisms.

Resilience today is not about preventing every incident. It is about taking the relevant preventive steps to keep the impact small, the disruption short and having the funds and services available to support recovery.

Alessandro Lezzi
Group Head of Cyber Risk
Beazley

Alton Kizzier
CEO
Beazley Security



Key takeaways

For insurance brokers

1 Cyber risk is systemic
Most firms underestimate the damage a ransomware attack or supplier failure can cause. Digital interconnectivity means insurance protection should consider multi-line impact, not just tech and data recovery.

2 Third-party and regulatory risks are growing
Even a single vendor compromise can halt operations. At the same time, regulations raise board-level accountability, creating greater governance and executive risk.

3 Technology amplifies opportunity and exposure
AI introduces new cyber, intellectual property (IP), reputational, regulatory and operational risks that organisations need to address and plan for as part of their tech transition.

4 Resilience is continuous, not one-off
Resilience now requires always-on detection and multi-department coordination. Insurance underpins resilience, but there are likely to be coverage gaps that firms need help to recognise and plan for.

For business leaders

1 Cyber risk is a strategic business issue
Systemic cyber incidents are rising, creating operational, regulatory and reputational impact, not just data loss. Their complexity and cost should not be underestimated.

2 Supplier and regulatory risks are growing
Greater interconnectivity across complex supply chains raises the risk of systemic disruption. Contracts, audits and continuity plans should anticipate these risks. Simultaneously, expanding and inconsistent global regulations create complexity and heighten executive liability exposure.

3 AI is a double-edged sword
AI boosts productivity and resilience, but it also adds new cyber, IP, reputational and regulatory risks that require careful management.

4 Stay ahead of tomorrow's threat
Reactive fixes are no longer enough. Today, forward-looking strategies that rethink risk capital allocation are needed. Insurance plays a vital role – but it is not the panacea – as gaps in cover need to be identified and planned for.

Key findings at a glance – 3,500 global business leaders' views

Cyber dominates risk worries

31%

selected cyber risk – data breaches, criminal threats and widespread outages – as their top risk concern, up from **29%** in 2025. Are the headlines resonating?

Data's regulatory fallout cyber concerns

23%

fear data loss and the regulatory repercussions, fuelled by an evolving and complex regulatory landscape.

Cyber resilience is being overestimated

78%

agree that they can **fully** recover from the financial and economic impact of a cyber attack, **82%** believe they are prepared for cyber risk. Certainty that may overestimate the reality.

Tech-led cyber security plans gear up

35%

are turning to AI investment to try and boost resilience as emerging threats hit home, while **33%** are upping cybersecurity spend – up from **24%** in 2024.

AI's economic promise inspires strong optimism

80%

agree that AI will boost their bottom line as the early buzz delivers tangible impact, and **72%** agree that it will replace jobs inside 18 months – up from **66%** in 2025.

Rising fears of falling behind the tech race

23%

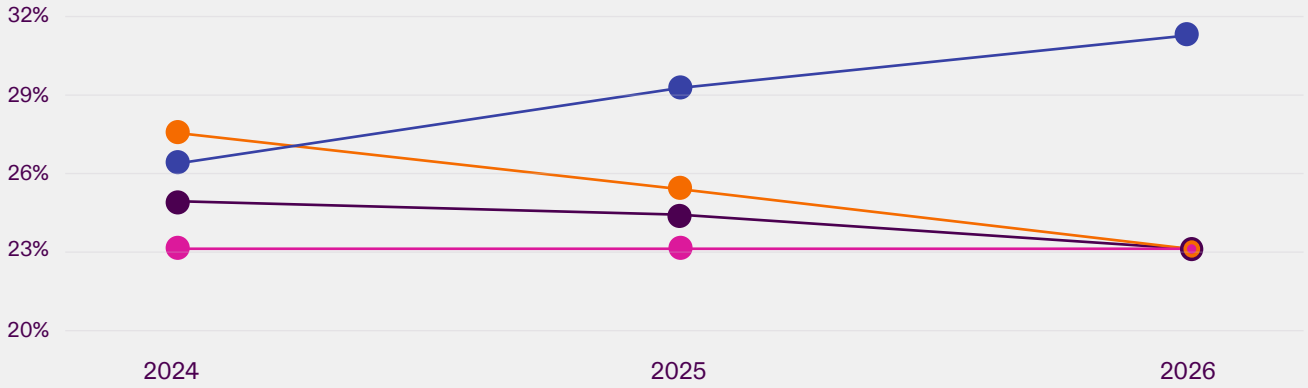
down from **24%** in 2025 – fear the risk of falling behind fast-moving frontier technologies and the opportunities they offer, and **23%** are also worried about the knock-on risks of legacy tech.

These statistics are taken from Beazley's Risk & Resilience surveys.

What the stats reveal

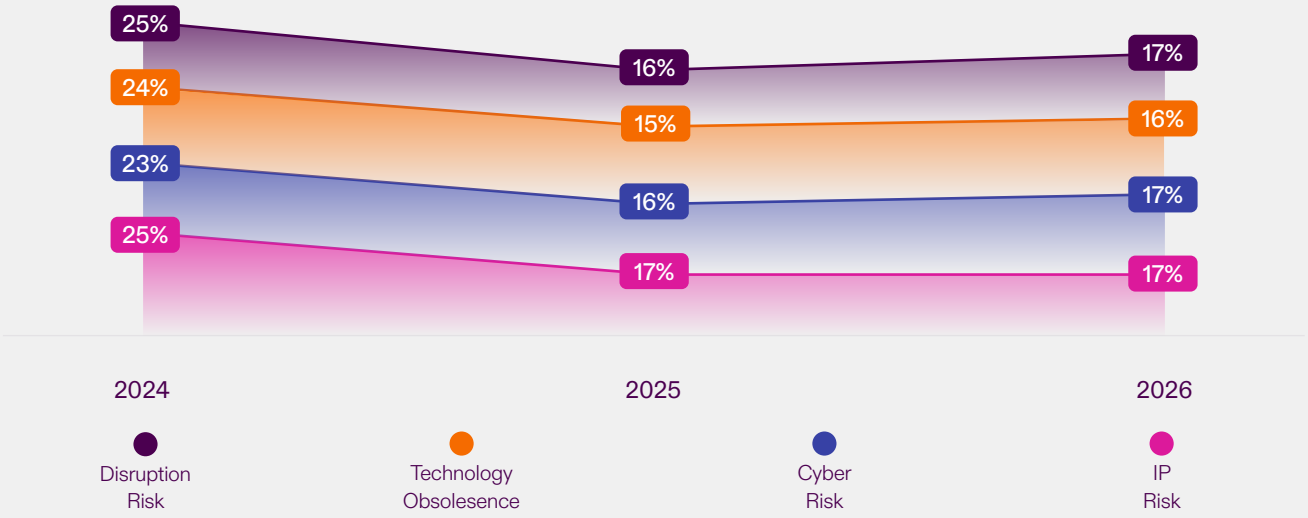
Risk over time

From 2024 to 2026, most cyber and technology risk categories showed a steady or declining level of risk concern, except cyber risk, which stands out as the threat that executives are most worried about. Tech disruption and technology obsolescence ease year-on-year, while IP risk concern stays flat throughout this period.



Resilience over time

Across all four cyber and technology risk areas, unpreparedness levels dropped sharply from 2024 to 2025, indicating perceived stronger resilience, but then level off or rise slightly in 2026. Overall, perception of preparedness remains significantly lower than in 2024, suggesting sustained, but slowing resilience confidence.



These statistics are taken from the Risk & Resilience Surveys undertaken in 2024, 2025 and 2026, with respondents based in the UK, US, Canada, Singapore, France, Germany and Spain. This year's survey was undertaken between 05.01.26 and 13.01.26, with the same year on year sample base. The resilience statistic is a combination of 'not very' and 'not at all' prepared answers combined.

Industry risk concern

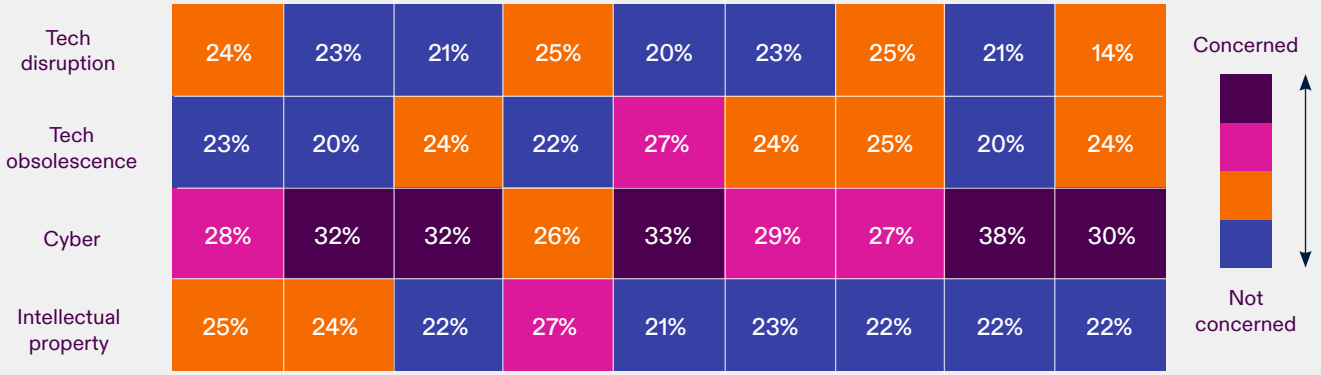
Cyber risk tops the risk concerns across all industries, notably across Tech, Media and Telecoms and Financial Institutions and Professional Services where data sensitivity and digital dependence peak.

Unease around tech disruption and obsolescence sit at steady, moderate levels overall, rising in Financial Institutions and Professional Services and the Public Sector – both still dependent on legacy systems built for bygone eras. Across the board, industries appear to rank IP risks at a similar level, though the stakes appear to be slightly higher for Healthcare and Hospitality firms where proprietary data is more essential for their success.

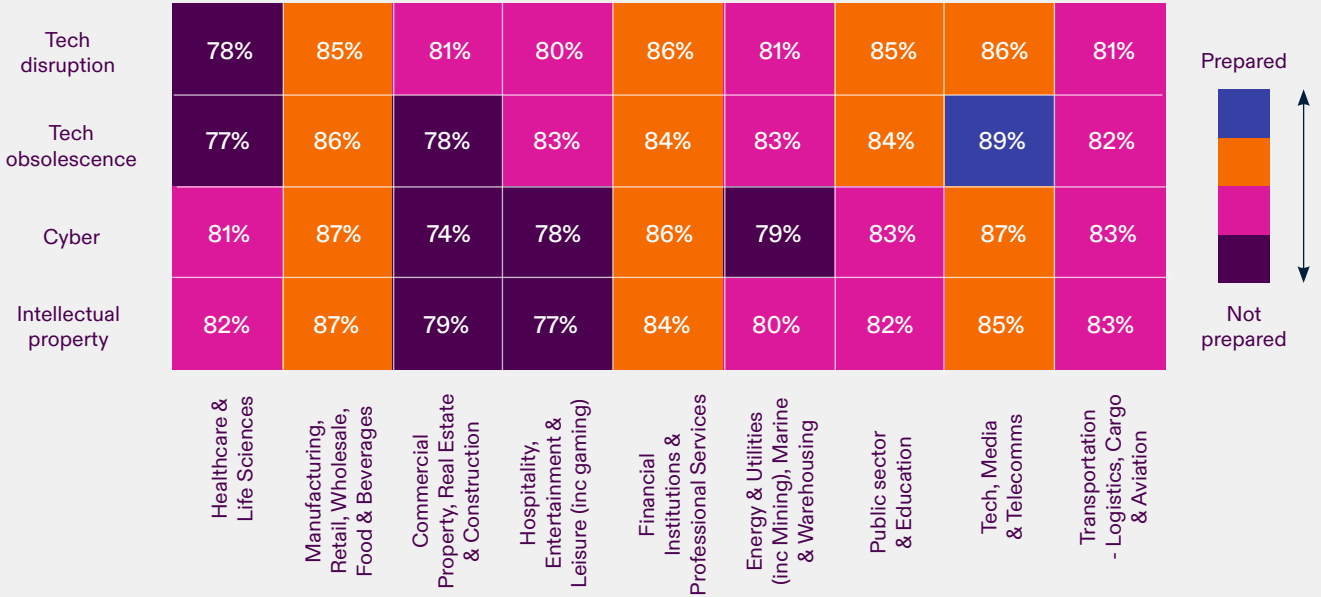
Industry resilience insight

Most sectors rate themselves highly prepared, especially Tech, Media and Telecoms, Manufacturing, and Financial Institutions and Professional Services. Commercial Property appears less confident. Healthcare wavers on disruption and obsolescence preparedness, Hospitality on cyber and IP. The headline is confidence, but beneath it, a growing mismatch between perceived resilience and real-world cyber and tech risk complexity.

How concerned is your industry about cyber and technology risk?

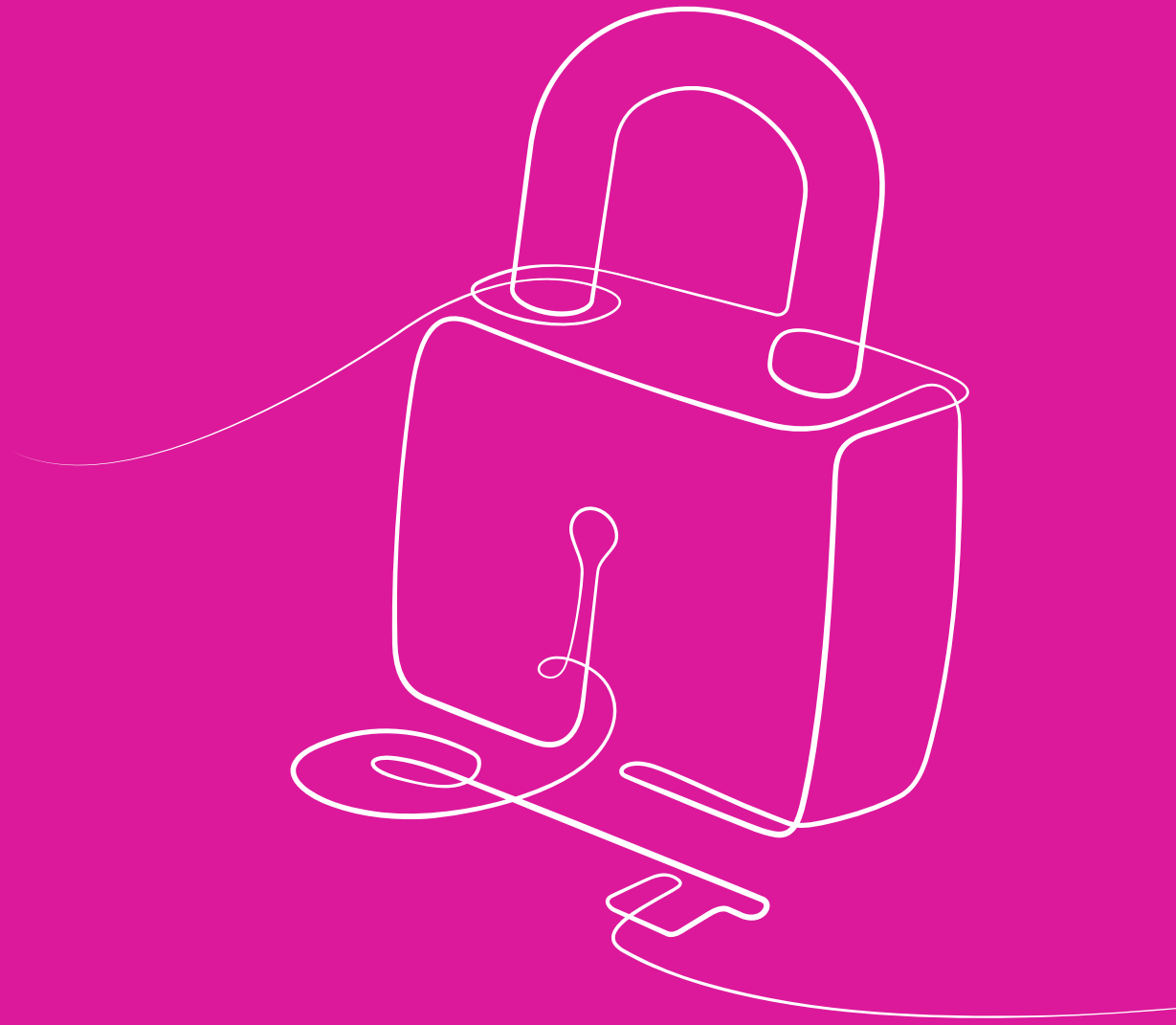


How prepared does your industry feel about cyber and technology risk?



These statistics are taken from the annual Risk & Resilience 2026/27 survey.

Contents



Beyond firewalls

Cyber attacks now trigger full scale operational crises

Today's cyber threats unfold as sustained operational crises, with lasting financial, regulatory, and supply chain fallout.

Leaders are overestimating their resilience

While executive confidence remains high, AI powered attacks are accelerating, exploiting basic weaknesses, and outpacing traditional defences.

Risk now spans data, partners and physical assets

With rising risks, intensifying data regulation and growing real world impact, businesses need full system visibility and stronger governance to stay resilient.

Charting an unwieldy cyber terrain

Cyber risk has widened its reach

It has shifted far beyond data breaches, yet our numbers tell a story of underestimation around the impact of these evolving attacks, which damage operations, drain financial viability, scar reputations and consume management hours.

2025 marked a year of hard lessons; it was the year we saw cyber attacks evolve into full scale crises – creating knock out blows that can buckle a business. A single breach can impact entire supply chains creating a domino effect that impacts customers, suppliers and shareholders, and in turn endangering the viability of countless individuals and enterprises. The damage is costly and complex to resolve and can last months and even years.

Businesses need a full view of risk and downtime costs to know what they can absorb and what must be insured.

AI scales attacks, downtime scales losses

AI is making cyber attacks easier, more frequent, and successful. Threat actors are using AI to run multiple, automated reconnaissance and phishing campaigns, each scouting thousands of organisations' systems for weaknesses to attack. With an estimated **82%** success rate[1], the scales tip heavily toward the attackers, leaving businesses racing to try and stay ahead.

78% of executives expect full recovery post a cyber incident.

82% claim cyber preparedness - revealing an underestimation of today's fast evolving cyber threat landscape.

Statistics from the 2026/27 Risk & Resilience survey

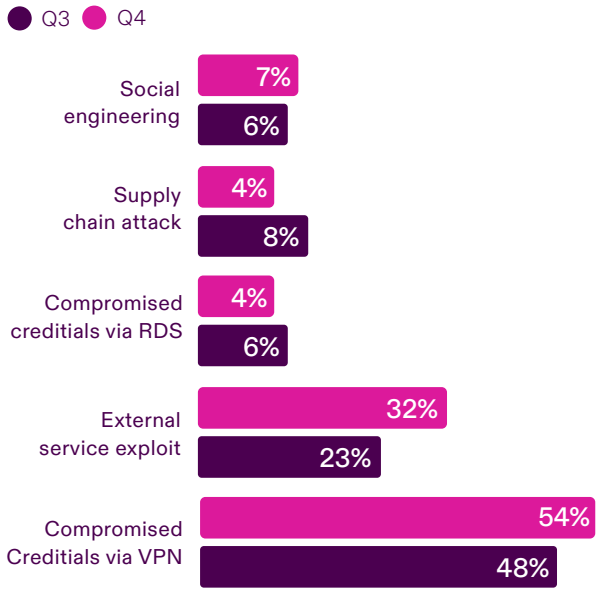
> **AI is enabling threat actors to operationalise their tactics and techniques more rapidly, making zero-day and n-day vulnerability exploitation more common. Time is critical. Organisations need to have continuous visibility, real-time exposure management, and strong incident response plans.**

Francisco Donoso
Chief Product and Technology Officer
Beazley Security

The reality of cyber risk

Threat actors follow the money, exploiting any opportunity to breach systems. Beazley Security's Q4 2025 Threat Report[2] found **54%** of attackers gained access via VPN-compromised credentials.

Ransomware initial access by category



Beazley Security Quarterly Threat Report, Q4 2025.

Cyber fallout: the long-tail impact of a cyber attack

When a ransomware attack hits a manufacturer

Breaches are fast - the fallout takes time

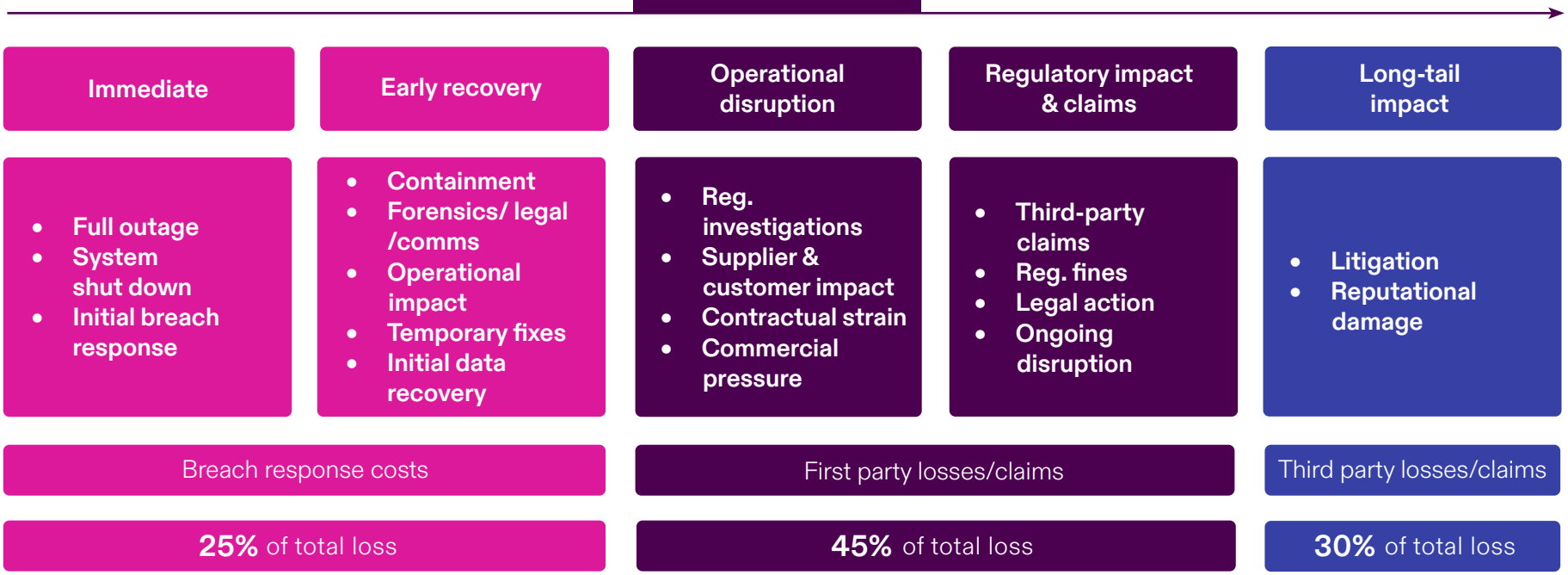
A ransomware attack on a manufacturer is not a one-day – it is a multi-month business crisis. An attack can trigger a full network outage, impacting operations and systems for weeks, months and even years.

Cyber attack

A typical ransomware attack on a mid-size manufacturer results in:

Average downtime **11.6 days***

Impact timeline **6-18+mths****



*On average, manufacturing companies lose $1.9 million per day to downtime from ransomware attacks - Comparitech.

**Time estimates are based on Beazley cyber incident handling experience.

The loss percentages reflect a typical ransomware attack on a manufacturing organisation and are provided for illustrative purposes only. Actual loss splits will vary depending on the circumstances of the incident, and attacks in other sectors or based on alternative data sets may differ significantly.

The new data danger

Data remains an attacker's goldmine, and we have seen a **50%** uptick[3] in stolen material placed online in the last quarter of 2025, with adversaries increasingly willing to ramp up public pressure when ransom negotiations stall.

AI-driven phishing attacks are using convincingly real messages, luring people into clicking malicious links that give cyber criminals network access. This deepfake activity targets people directly, and can result in ransomware attacks that lock down entire operations.

Risk and regulation – a perfect storm

On one side, malicious cyber attacks are ramping up, on the other, regulators are amplifying scrutiny to combat emerging cyber risks that affect people, infrastructure and national security.

In parallel, AI competition has morphed data into a powerful geopolitical lever in the race for technological leadership and economic strength. Governments are asserting control, unwilling to allow fragile data ecosystems to turn into pipelines for foreign exploitation and criminal misuse.

Yet the rules governing that data differ from one country to the next, creating onerous obligations that collide, and tying cyber risk to questions of national policy. A single system may fall under several privacy and security laws at once, depending on the jurisdictions it operates in.

Fragmented rules are a cost multiplier

Inadequate and misaligned data governance could unleash regulatory backlash – from forced disclosures to enforcement, along with hefty financial penalties. This can then affect access to insurance and legal recovery pathways, affecting viability and growth. In this environment, legal and regulatory alignment must rank high on a business' strategic agenda.

Divergent regulations are increasing pressure on every business decision. With a globally aligned cyber data framework still out of reach, fragmentation is driving unnecessary cost and complexity - even for well-governed organisations.

Data risk is no longer a standalone issue

Data risk now sits at the intersection of technology, regulation and geopolitics. Treating it as part of core governance – rather than a specialist issue – enables not only fast incident responses but helps firms stand up to regulatory review and prevent costly clashes between competing international requirements.

75% of business leaders selected data loss and regulatory reporting as their top cyber risk impact concern.

Statistic from the 2026/27 Risk & Resilience survey.

Supply chain vulnerabilities

Reliance on shared or a third-party provider software widens an organisation's vulnerability 'perimeter'. Verizon's 2025 Data Breach Investigation Report shows third-party involvement in 30% of breaches[4] – roughly double the year before.

This proliferation stands as clear evidence that inaction is untenable – businesses must manage supplier side cyber risks actively.

> **"Threat actors are targeting SaaS vendors, and third-party suppliers, and the developer ecosystem, using them as a gateway that provides a faster path into a multitude of other potential victims.**

Francisco Donoso
Chief Product and Technology Officer
Beazley Security

From blind spots to early intervention

There are solutions available that identify hidden supply chain vulnerabilities across vendors and third-party tools. Combining enterprise mapping with real-time risk monitoring provides a 'live' view of supplier threats and potential system-wide failures helping teams to intervene early to prevent external weaknesses from causing internal disruptions.

Managed extended detection & response (MXDR)[5] and exposure management services[6] can help firms to stop just waiting for the next hit. They are looking to move past reactive patching by eliminating blind spots and vulnerabilities early and achieving always-on visibility across their network.

> **Our approach to exposure management provides an early alarm system that spans client environments, including their integrated suppliers. Always on, this provides up-to-date visibility, along with insights and guidance on the level of risk and what to do about it. This is a leap forward in ecosystem risk management.**

Raf Sanchez
Global Head of Cyber Services
Beazley Security

The basics still matter – but they must not be standalone

In practice, when the basics are done well, the impacts of incidents can be tempered: strong authentication, tightly managed privileges and fast containment when credentials are stolen or used. Weak or absent multi-factor authentication (MFA) remains a core point of exposure.

The basics only hold if the wider ecosystem holds with them, and when these foundations are weak or uneven across partners, a business can take blows in corners they thought were under control. To bolster supply chain resilience, boards must take the pragmatic path. This means staying alert to the fact that vulnerabilities often still sit in the well known routes attackers continue to rely on.

Cyber lapses with physical stakes

Digital attacks increasingly have real-world consequences – particularly in sectors such as marine and property.

GPS spoofing, for example, as seen recently in the Straits of Hormuz, is rising sharply. By broadcasting counterfeit signals, attackers can manipulate a vessel's perceived location, potentially causing:

- Groundings
- Collisions
- Lost or damaged cargo
- Environmental damage

A vessel in distress needs a marine response; a system breach needs cyber forensics. Operators now seek support that delivers both, knowing how easily digital threats can disrupt vessel operations. It requires aligned operational, safety, and cyber teams - and partners who understand that cyber incidents at sea have real-world consequences.

> **Effective cyber risk mitigation is rarely exotic: it should start with basic cyber hygiene and system recovery fundamentals. Firms must prepare to manage multiple claims that can cascade from a single incident, such as operational disruption, ransom demands, regulatory investigations and floods of claims from customers, suppliers and shareholders.**

Mark Singer
Claims Focus Group Leader, Cyber
Beazley

It's time to brace for unrelenting threats

Cyber risk has outgrown traditional defensive perimeters. Today's threats – fuelled by AI, geopolitics, regulatory fragmentation, and interconnected supply chains – spread faster, strike harder, and last longer than many business leaders expect.

The fundamental risk mitigation steps still matter, but they're no longer enough on their own. Resilience today demands a full system, always-on view – across data, partners, infrastructure and jurisdiction – because today's threats spread faster, hit harder, and linger far longer than global executives appear to be anticipating.

Case study: Small businesses, big exposure

The scale of the problem

As economic uncertainty persists, cyber risk grows. Online fraud is rising as AI-enabled phishing using social engineering becomes more advanced, while redundancies raise the risk of insider threats from disgruntled employees.

Cyber crime impacts roughly five million victims annually in England and Wales, with technology involved in over half of reported crime. And yet only 1.7 million report cyber incidents to the police, 87% of cases are closed immediately, and 98% result in 'no further action'[8]. Less than 1% of law enforcement resources are allocated to cyber crime[9], limiting investigative capacity.

For sole traders and small businesses the need for strong cyber security has never been greater. Many operate through personal devices, shared logins and standard operating software, making them easy targets for cyber threat actors and more sophisticated cyber criminal gangs.

The risks are numerous and wide-ranging, The Cyber Helpline - a charity offering free, expert cyber advice for individuals and sole traders in the UK and US[9] - sees cases that typically fall into three classifications:

- **50%** digital fraud and scams – including investment scams, job fraud, impersonation.
- **25%** technical cyber crime – such as ransomware, hacked devices and accounts.
- **25% human-centred harm** – for instance cyber-bullying, harassment, sextortion, intimate image abuse.

The impact of an attack goes far beyond financial loss, hitting personal lives as well as business operating systems.

> **Cyber attacks are personal and the perpetrators are masters at finding a weak point. For victims, the biggest impact is rarely the financial loss, it's the impact on their mental health and on their ability to operate online afterwards. They feel anxiety, fear, depression and a shattered sense of security, especially in the digital space, which can cripple their ability to continue effectively.**

Rory Innes
Founder and CEO
The Cyber Helpline

A breach that shut down a business

In one case, a former employee of an award-winning spa accessed its systems, deleted the client database and business records, and launched an online hate campaign against the owner. With no way to contact clients and run the booking system the firm's reputation was damaged, business dwindled and the spa eventually closed.

Critical support exists

Help is available, but it's fragmented, difficult to navigate and often unknown to the people who need it most. Assistance typically falls into three categories:

1. Free specialist help for immediate guidance
From international bodies to national agencies, resources exist to help small businesses with cyber issues. Ranging from (but not limited to) free guidance and training to threat reporting, performance goals and incident response support.

For example:

- **UK:** National Cyber Security Centre (NCSC)[10]
- **US:** Cybersecurity and Infrastructure Security Agency (CISA)[11]

2. Commercial incident-response services
When deeper technical work is required - such as forensics, malware analysis or data recovery – small to medium-sized enterprises (SMEs) can access private sector incident response.

However, costs typically start at tens of thousands of pounds, making this inaccessible without insurance.

3. Platform-level support
Many attacks involve compromised accounts on major platforms. Providers such as: Microsoft, Google, Shopify and accounting and payment systems offer recovery tools, account security features (including MFA) and fraud response pathways. But many small businesses simply don't know these services exist.

Building resilience

For small businesses and sole traders, the truth is stark: today's cyber risk landscape is more complex, more aggressive and more unforgiving than ever.

Despite escalating threats, many believe they could recover quickly.

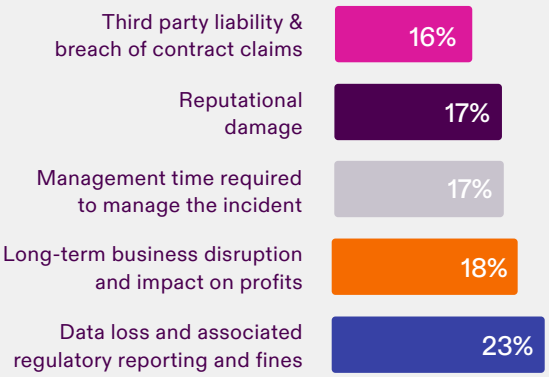
73% of SMEs say they're confident they could fully recover from a cyber attack.

Beazley Risk & Resilience survey 2026/27

But the gap between perceived and actual resilience remains wide. Given the accelerating speed and variety of risks, they appear to be underestimating their true exposure.

The impact of a cyber attack extends well beyond data loss – management time, business interruption and lost income are likely to be equally as damaging.

Perceived impact of a cyber incident by small businesses



2026/27 Risk & Resilience survey

Practical resilience for small businesses

The following steps can prevent panic, limit escalation and accelerate recovery when an incident occurs.

1. Raise the baseline: essential, non negotiable security controls

Simple, default security measures dramatically reduce risk:

- Multi-factor authentication (MFA)
- Strong, unique passwords
- Proper off boarding processes
- Regular, separate data backups
- Access controls and basic system management

2. Make cyber insurance a core part of resilience

For small businesses with limited resources, cyber insurance provides access to structured, expert support, including:

- 24/7 incident response
- Forensics and investigation
- System restoration and data recovery
- Legal and regulatory guidance
- Crisis communications
- Business interruption cover

Insurance transforms a chaotic, self-led crisis into a coordinated, expert driven recovery.

3. Normalise preparedness

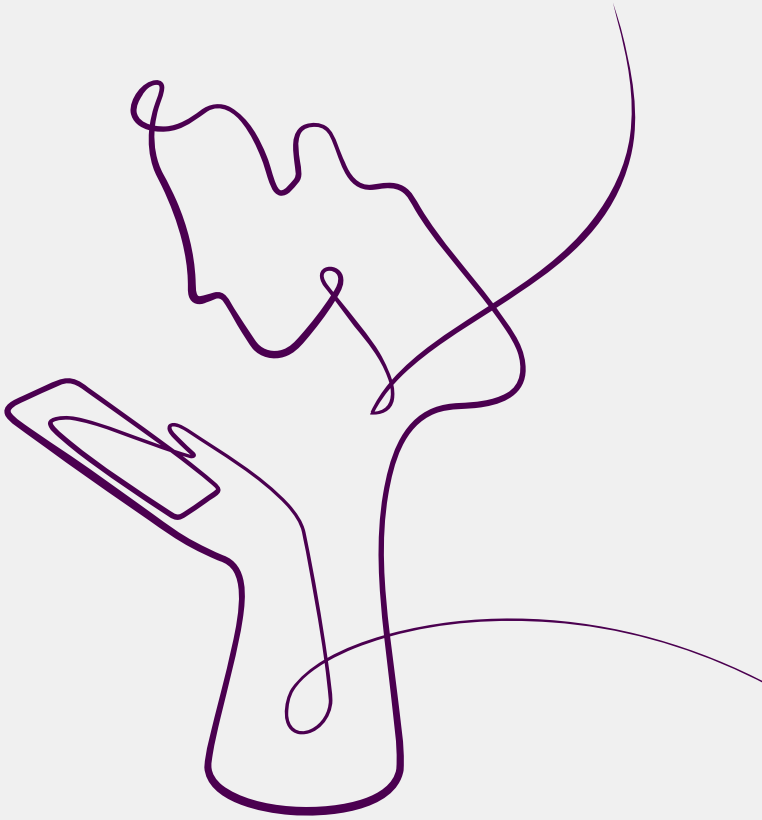
Resilience is not just technical. It's behavioural:

- A simple one-page realistic actionable response plan
- Awareness of free and insured support pathways
- A culture where reporting mistakes early is encouraged

The bottom line

Cyber risk is rising fast, but small businesses can protect themselves to reduce cost, stress, downtime and long-term damage.

Cyber insurance with integrated support services helps firms improve their basic cybersecurity. It offers advice on preparing for attacks and access to specialists to manage and recover from incidents, reducing disruption and strengthening long-term resilience.



Behind the hype

AI is transforming operations at speed, unlocking major gains in efficiency and decision making

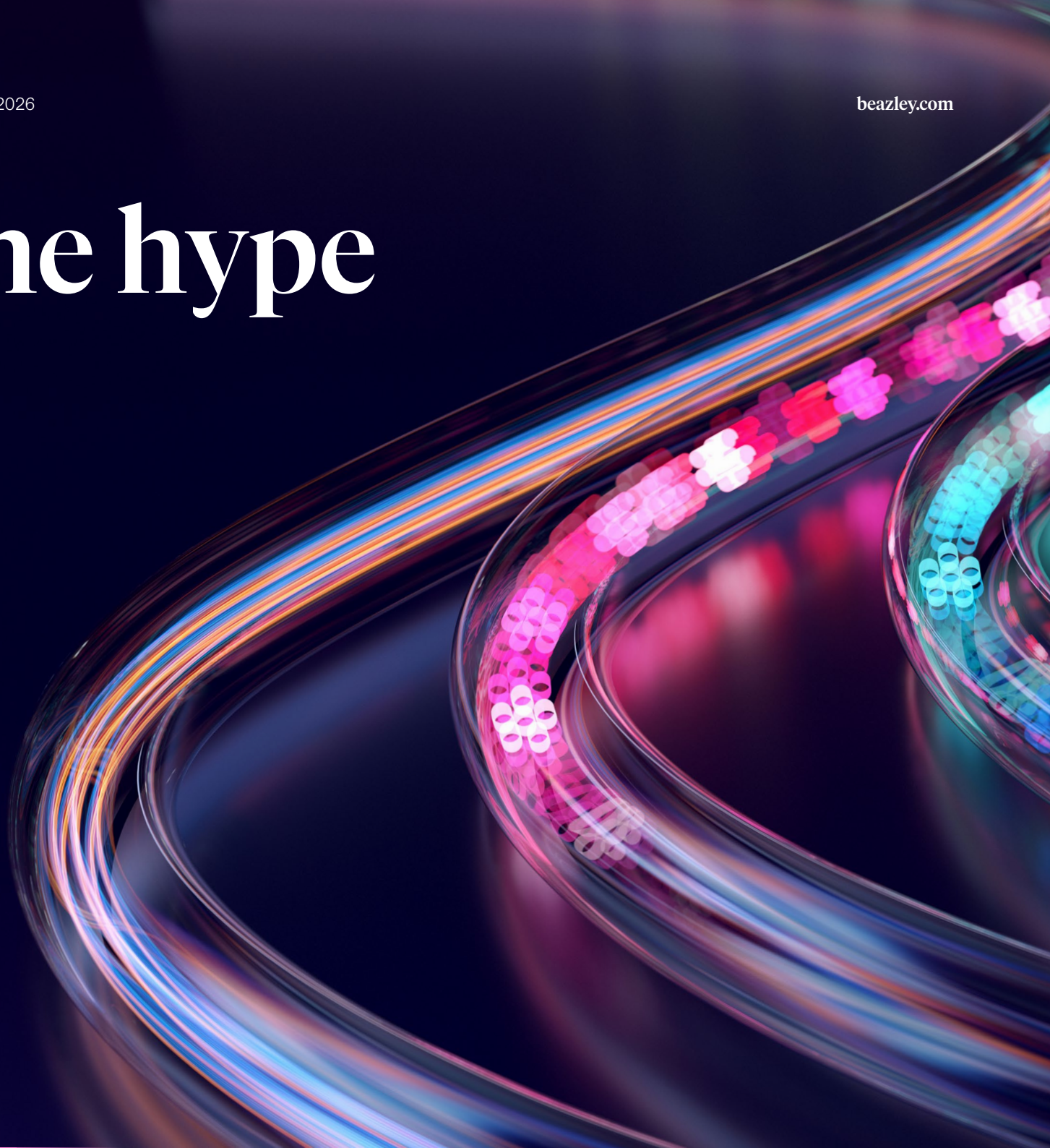
It is also introducing systemic risks that can spread fast across an organisation's network.

Threat actors are using AI to supercharge cyber attacks

Overwhelming traditional controls and widening the attack surface as businesses adopt agentic systems and interconnected tools.

Governance is lagging behind innovation

Making clear guardrails, human oversight and stronger accountability essential as AI becomes a critical dependency across entire ecosystems.



Unpacking the AI paradox

Rapid adoption, rising exposure

Businesses are adopting AI at unprecedented speed, while regulation struggles to keep pace. Beyond the hype lies a complex reality – the good, the bad and the ugly of AI.

Agentic AI carries promise and pressure in equal measure. For businesses, the benefits are already clear. These systems speed up operations, boost efficiency and tackle problems previously deemed unsolvable.

But with this power comes risk. Errors can escalate, biases can impact decisions, answers can be unpredictable, and exposure to cyber threats and extortion grows. Organisations need to stay ahead of both the opportunity and the risks.

Cyber attackers have also woken up to AI's potential. Threat actors are using AI to supercharge the speed and success of their attacks. This threat surge risks overwhelming existing oversight and security controls not built for threats evolving this fast.

The speed of AI adoption is astounding. Gartner predicts that one-third of enterprise software will include agentic AI by 2028, with the technology already making 15% of daily autonomous decisions[12].

Global use is certain, so firms need to balance these new capabilities by actively managing the extra risks they create.

The good

The opportunity is clear: where earlier automation sped up tasks, agentic AI systems speed up decisions and connect processes once slowed by people, policy, and friction.

Workflows move more smoothly with fewer pauses and handoffs. Firms operate with a level of continuity that previously felt out of reach, giving teams more room to focus on growth and revenue.

When cyber issues surface, AI defence models can spot and respond to them at machine speed – identifying them before most teams start their day and containing them before they escalate.

Through vibe coding[13]: agentic AI creates code by turning vague ideas into working results through filling in the details itself. AI systems can read, build and test concepts faster than a person can even open a file.

Work that once took weeks now happens in minutes. This speed allows teams to explore more ideas and use complex technical tools that previously required years of expert training.

Merriam-Webster and Collins Dictionary have already noted this shift, with the latter naming vibe coding the Word of the Year for 2025[14].

Used with intent: AI becomes more than a tactical add on. By utilising AI agents and other new developments, it can function as a built-in structural management system that supports how a whole organisation works.

80% of our surveyed global executives expect AI to have a positive economic impact on their business.

35% of executives plan to invest in AI to improve business resilience.

Statistics from the 2026/27 Risk & Resilience survey.

> **While AI is helping improve attackers' capabilities, it also gives defenders the chance to get ahead. By automating risk discovery with agentic testing and investigation tools, we can identify, validate and contain threats before attackers exploit them.**

Francisco Donoso
Chief Product and Technology Officer
Beazley Security

The bad

Risk rises in tandem: AI systems can have built-in flaws: they can be biased, invent false information, hallucinate or even lie, and often operate as 'black boxes' where their decision-making is unclear, hard to interrogate and sometimes incorrect. Because they are autonomous and highly connected, a single error can spread through an entire network.

Natural language prompts: The same speed that makes vibe coding useful – where AI guesses what you want from loosely defined prompts and does the rest itself – also makes it dangerous. AI agents can produce results that look finished but contain hidden errors, flawed assumptions and missing safety checks. It also can open the door for cyber criminals, as generic coding patterns are easier to exploit. New security risks also emerge when these systems read emails or messages – a single line of hidden text in an inbox can trick an AI into taking the wrong action.

Unintended consequences: Automated tools can accidentally connect systems that were meant to stay separate, creating unintended pathways for data leaks or attacks. Give an AI agent too much autonomy, and a single flawed or manipulated response can trigger damage – deleting files, leaking data or exposing critical systems it has 'the keys to the house.' Criminals exploit this too, using free AI tools to probe and attack company weaknesses. OWASP flags this 'Excessive Agency' as an emerging security threat for 2025–26[15].

Weaknesses in external vendors can cascade across the whole ecosystem, while a company's own AI missteps can compromise partners downstream.

When oversight lags behind, employees can turn to unapproved, unmonitored 'shadow AI'. Zendesk reports shadow AI use growing by up to 250% in some sectors[16].

Threat exposure: When AI agents connect to an organisation's systems, the 'attack surface' – the number of ways a cyber criminal can get in – grows significantly. Managing how data enters and leaves these systems is now a top-tier business risk.

The UK Government's Code[17] of Practice for the Cyber Security[18] of AI warns that standard security programmes may miss specific AI threats like data poisoning (corrupting training data) and prompt injection (tricking the AI with malicious instructions).

These risks are even more dangerous when an AI's output can automatically change user permissions, trigger payments, or make customer decisions.

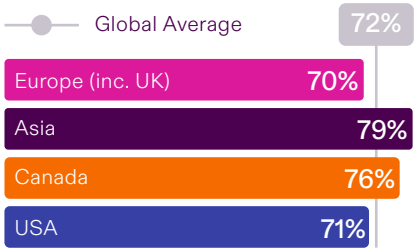
Geopolitical fallout: Automation risks more than just your tech. When AI takes over too much work, it can gut entire teams, killing morale and trust. This often leads to staff checking out or resisting change, which makes the company slower and weaker when a real crisis hits.

In extreme cases, mass job losses could trigger social unrest and public backlash. This will bring heavy pressure from regulators and unions, turning a business shift into a public disaster.

> **AI is accelerating attacker capability – from faster vulnerability discovery to more efficient targeting and exploitation. It's a powerful vulnerability finder for defenders too, but it cuts both ways: the same techniques that surface hundreds of overlooked flaws in widely used open-source components can be used to prioritise and scale attacks.**

Melissa Carmichael
Head of Cyber Risks
Beazley

Workforce transformation



Percentage of executives who agreed that AI will lead to job losses in the next 18 months in the 2026/27 Risk & Resilience survey.

The ugly

Deepfake deception: AI imagery has evolved beyond simple filters. Systems can now generate entirely fake photos of leadership teams, staff, or buildings that look real. These fakes are often placed into presentations, news articles, or social media profiles to trick investors and the public. In some cases, scammers have used fake internal screenshots to create false evidence for legal disputes.

Fake-voice fraud: Voice cloning is an increasing threat. With just three seconds of recorded speech, an attacker can clone an executive's voice with roughly **85%** accuracy[19]. These clones are used to call employees and authorise fraudulent money transfers that sound completely legitimate. A McAfee survey found that one in four people have encountered an AI voice scam, and **77%** of those victims' lost money[20].

Sextortion: Entire playbooks and boiler-room operations now exist online, teaching criminals how to coerce victims with maximum impact. Executives, non-executives, business owners, and even their families and networks, are being targeted to breach larger organisations or force ransom payments by exploiting personal – not just corporate – weak points.

A single scam might combine a deepfake video call, a cloned voice message and a follow up email – all created using off-the-shelf AI tools.

For criminals, the cost of these attacks is low, but for organisations and targeted individuals, the damage is severe.

The way forward

Company boards and policymakers must prioritise governance. They need to recognise that while automation increases efficiency, it also introduces hidden vulnerabilities.

These risks are most damaging when AI agents handle a company's core operations, such as finance, purchasing and identity management. If these systems fail, the fallout can destroy a company's reputation, break partnerships and lead to legal action. Firms must be cautious.

Autonomy inside guardrails

Clear rules on when to pause automation are essential. At certain high-risk points, the AI must stop and hand control to a human. This ensures that while automation makes security faster, humans provide the final oversight needed to prevent a technical glitch or error from becoming a major crisis.

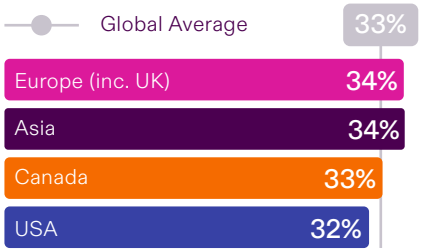
Automation board oversight should include 'bounded autonomy' architectures that:

- Include explicit permissions: that limit what an agent can do (for example: it can read a file but not delete it).
- Step-up approvals: require a human to sign off on high-impact actions, like large financial transfers.
- Safe default states: program the agent to stop and ask for help if it is confused or its confidence is low.

Ultimately, AI risks are beyond being mere technical bugs; they are issues of design, control and accountability that leaders must manage. The most resilient companies will be those that treat AI as a critical dependency. This means building firm guardrails, improving visibility and ensuring that humans stay accountable for automated choices.

AI risk concern by region

AI-led tech disruption, including bias, non-performance, system obsolescence and operational impact.



Percentage of business leaders who selected this as their top macro factor of particular concern in the 2026/27 Risk & Resilience survey.

> **AI adoption is scaling fast, but governance is lagging behind. New tools and custom integrations appear overnight, yet compliance duties don't slow down. The organisations that win will set clear boundaries for what systems can do, keep auditable decision-to-action trails, and build controls that scale with change.**

Craig Linton
Head of US Underwriting Management, Cyber
Beazley

Case study: Tech that protects

Safety-by-design AI to pre-empt protection

Firms are rushing to adopt AI as they chase productivity and fear obsolescence. Yet excessive autonomy can create widespread damage across company operations, all because they're able to act with carte blanche within company systems.

The right guardrails can keep their behaviour safe and contained so that firms can pursue their productivity and growth goals safely and with confidence.

Online safety tools and frameworks are a real-world illustration of how guardrails let autonomous AI operate safely when it is supervised and designed to prevent harm before it spreads.

The human cost of digital harm

In the world of online safety, a proactive stance is essential – predators and malicious systems deliberately seek out vulnerable users, especially children, exploiting their trust or lack of experience.

Some **80%** of children across 25 countries feel at risk of sexual exploitation or abuse online[21], while deepfakes are accelerating the threat: last year, **1.2 million** children said their images were turned into sexually explicit deepfakes[22]. With harmful content spreading in seconds, reactive methods mean the damage is already done.

The pressure is not only on victims: over a quarter of content moderators experienced moderate to severe psychological distress in 2025, with another quarter reporting low wellbeing[23].

Guardrails that hold under pressure

Where cybersecurity defends infrastructure, 'safety tech' defends people[24]. It can intervene in real-time – blocking, flagging and removing harmful content as it is created or shared – by combining age assurance, automated detection and high-confidence intervention. By targeting the key moments, it can break the chain of harm before it can start[25].

Two examples demonstrate the real-world application of safety tech and online safety principles:

Ofcom's guidance on 'highly effective age assurance': sets a clear bar for how age-assurance systems should block children from reaching harmful or adult content[26]. 'Highly effective' age checks must be: accurate, fair, and reliable; approved methods include: AI facial analysis, ID-to-selfie matching, secure digital wallets. These tools must work every time – balancing child safety with adult rights and privacy.

Automated detection of child sexual abuse material (CSAM) can catch illegal material before it spreads[27]:

- Hash-matching blocks known illicit content at upload.
- Machine learning classifiers flag new or previously unseen material instantly.
- Reviews happen in milliseconds, not hours.
- Automation protects human moderators while enabling large-scale compliance.
- High-impact decisions have human approval.

For businesses, these examples reveal the value of governed autonomy when the stakes are high.

Fewer mistakes, breaches and headaches

Businesses can replicate these principles by introducing clear, embedded security controls for their AI-powered enterprise agents, shaping a secure approach for how these automated systems operate.

Whenever agents handle financial transactions or sensitive records, the goal is proactive prevention – the system must block risky actions before they can cause a failure, a breach or an action that falls outside compliance. This looks like:

- **Clear permission rules:** that restrict access and actions to verified individuals.
- **Step-up reviews:** that escalate any high impact AI action to a human approver before it can go ahead to minimise the risk of high-impact errors.
- **Safe defaults:** that mean when a system cannot make a confident, low-risk decision, it automatically defaults to its safest setting or halts actions completely.
- **Transparent audit trails:** that ensure a defensible, logged record of actions and activities, strengthening accountability, regulatory compliance and reducing legal exposure.

The benefit is a more controlled environment with stronger corporate governance and consistent compliance. Financial errors are stopped before money moves, sensitive data stays protected, audit trails stay clean and teams spend less time repairing avoidable mistakes.

These guardrails create confidence, enabling organisations to expand the use of automated AI safely.

Resilience reimagined

Resilience must shift from a one-off exercise to a daily discipline

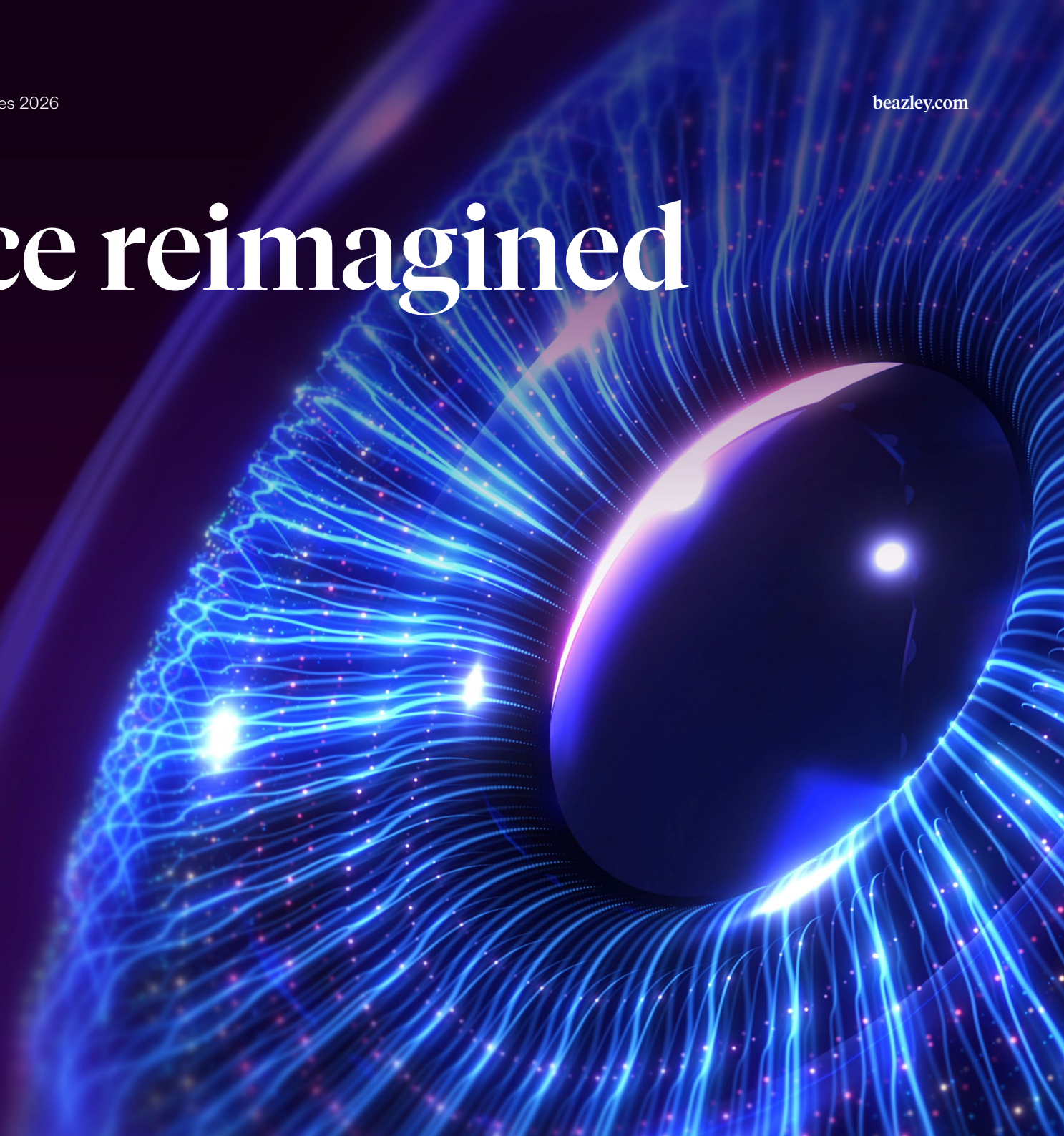
As interconnected systems, AI adoption and geopolitical tensions make disruption faster, broader and harder to contain.

Most firms are overestimating their ability to recover from a cyber incident

Revealing dangerous blind spots as cyber attacks, system failures and supplier outages trigger cascading operational and financial damage.

True resilience means pairing preparation, practical planning and fit for purpose insurance

So organisations can absorb hits to operations, minimise downtime and manage crises that partners or policies alone don't cover.



It's time for unyielding preparedness

Reassess readiness

Today's connected world demands constant, all-round protection. This requires rethinking resilience so that organisations are alert to, and prepared for, threats that could impact their networks, operations, physical sites, reputation or finances.

The whirlwind evolution of technology is turning into a test of a firm's capacity to keep its systems steady and safe. There are two types of firms on either side of this coin, and both are exposed. One side may be overestimating its readiness, the other knows it's not ready at all – but urgency applies equally to both.

Either way, the damage doesn't wait for a firm to catch up. Risks hit core operations, and spotting them late makes them nearly impossible to stop and can even bring businesses to a halt.

Resilience from every angle

Resilience needs to become part of the daily build – broad and continuous and shaped through routine decisions, not a measure taken only when pressure arrives. It means planning ahead, understanding where the greatest costs might surface, and zeroing-in on where insurance and controls may fall short as technology-driven risks expand.

The increasing interconnectivity of systems and use of AI creates rising risks from digital and human error, and intensifies cyber attacks, especially as technology and geopolitics evolve. Preventing every attack is now impossible.

Realistic planning drives recovery

An organisation's level of preparation is the thing that will define its recovery when an incident happens.

Every area of an organisation must be included in crisis plans and preparation, and the plans must be practical and realistic as to how an incident might unfold. With the right insurance partners and risk plans already in place, the impact can be contained – making disruption shorter and easier to manage when it hits.

Plot the true costs and loss

The cost of a cyber incident evolves over time, often in ways not immediately visible. Initial losses, disrupted operations or paused production lines may seem contained, but these early-stage figures often underestimate ripple effects across suppliers, contractors, and dependent systems.

As the days and weeks pass, the situation often intensifies. Executive leadership bears a heavy toll as they are pulled into long stretches of crisis management – deciding on ransom response, handling regulatory responses, managing communications and directing system shutdowns to limit damage. Meanwhile, fixed costs continue as usual, even when revenue drops to zero. The gap between short-term disruption and long-term financial loss becomes wider with every passing day.

For some, revenue stops entirely for weeks while fixed costs continue to accrue, revealing how much heavier the long-term consequences can be compared to the first wave of disruption.

> **"The financial consequences of cyber incidents often outlast technical recovery, which is why clarity on business interruption exposure is essential. Boards need to quantify downtime by critical process, test recovery assumptions and treat resilience as a business metric, not a security score. Because duration drives real loss.**

Ben Hobby
Partner, Baker Tilly
London

78% of executives are confident in a full, post-attack recovery, but confidence without capability is only sentiment.

Statistic from the 2026/27 Risk & Resilience survey.

Interconnected risks

Sprawling digital ecosystems and interconnectivity can turn shared systems into shared vulnerabilities. And weak links in the chain often determine the outcome. For example:

- **CrowdStrike outage[29]:** In July 2024, a single flawed software update crashed 8.5 million Windows devices globally. This 'logic error' caused the 'blue screen of death' for banks, hospitals, and airlines, resulting in over 10,000 cancelled flights and roughly US$5.4 billion in losses for major companies.
- **Cloudflare[30]:** In November 2025, a system fault crashed company software responsible for several services. An auto-generated configuration file exceeded its size limit disrupting access for millions across platforms including Canva, X and ChatGPT .

Significant disruptions in recent years in companies such as Microsoft and AWS also highlight how failures in hyperscale cloud environments can rapidly cascade across dependent organisations.

Many firms rely on 'just-in-time' supply chains and tight cash flows, which can fail when a supplier's software error or a digital contagion spread. If a partner is compromised and data is corrupted, the impact hits a firm's workforce and production immediately – production stops, customer deliveries fail and cash flow dries up.

External providers are unlikely to cover the associated losses of a system glitch or attack. Many firms now have tight terms and conditions that limit their liability for outages or business interruption. This leaves impacted organisations having to pick up the cost.

Cyber shocks hit small firms harder

Smaller firms are even more fragile, relying on credit and thin reserves, so even brief downtime can tip them into critical danger. In a cyber event, where systems can be locked or payments stopped instantly, these limits turn technical disruption into liquidity risk.

Government programmes such as the UK's NCSC Cyber Assessment Framework and Cyber Essentials[30] aim to raise baseline resilience. But the need for insurance remains since many smaller firms still lack the capability, tools or financial room to apply these standards consistently.

Assessing your armour

Resilient firms assess their exposure, test their assumptions and build strength across every department. This requires coordinating policies, governance, detection and response plans across IT, operations, finance, HR, legal and the entire supplier network.

A complete view of risk, combined with the discipline to act, keeps organisations in control as technology and threats move faster.

The fact that our Risk & Resilience 2026/27 survey reveals that 78% of global executives report full confidence in their organisation's financial recovery post a cyber attack, only goes to show the proliferation of dangerous blind spots. Rose tinted assumptions about whether they are a likely target, or how much they could lose in a severe cyber event, leaves firms vulnerable to the worst outcomes. To not get caught in underestimation, firms must treat resilience like a feedback loop instead of a one-off fix, to help recovery become faster, cleaner and far less costly.

Lack or inappropriate levels of cyber insurance post an attack or major internal malfunction can be construed as a breach of fiduciary duty by company directors, potentially leading to claims against the directors and officers of the impacted firm.

> **"In the US, you can bring a shareholder derivative action without a stock drop by claiming directors breached their fiduciary duties around cyber preparedness. But a securities class action is fraud-based and requires a stock drop – which usually follows a major cyber breach.**

Wiliam Clarke
Claims Team Leader
Executive Risk
Beazley

Insurance is a bridge between preparation and recovery

Insurance should support – not replace – operational readiness. Even with strong controls like MFA and fast patching, organisations remain vulnerable. AI-driven social engineering is increasingly convincing, enabling attackers to bypass MFA and exploit human error.

In late 2025, nearly half of successful breaches impacted accounts had MFA enabled, and zero-day flaws were exploited before mitigation was possible[31]. Breach tools and techniques have grown in sophistication and accessibility, pervasive global instabilities have increased the impetus to attack, and tech disruptions are spreading further and faster. These risks cannot be fully controlled. This makes risk transfer an essential safety net to limit the severity of the impact on finances and operations.

From policy to preparedness

Today's value-added services incorporated into cyber policies offer, for example expert insight, giving access to vital services that can help organisations to prepare, manage and recover from cyber incidents.

Firms that match their coverage to realistic recovery times, test their plans and assumptions continuously, and make insurance a core part of their resilience strategy can act faster during a crisis.

29% of executives plan to explore insurance options with risk and crisis management.

Statistic from the 2026/27 Risk & Resilience survey.

Mind the gap

Insurance provides the tools, experts and funds to recover from a cyber attack, but it cannot cover every risk. Scenario planning with clients, brokers and underwriters can help to map out worst case scenarios and identify where existing insurance policies might fall short, enabling more tailored solutions to be created.

These are some common insurance gaps that should be considered:

- **Boardroom liability:** A directors & officers liability (D&O) policy may cover the organisations' or board members' response to an attack, but new exclusions for confidential information or cyber hygiene failures could limit protection.
- **Ongoing fallout:** Cyber insurance covers the immediate breach and recovery, but the long-term costs – such as reputational damage or future business loss – have the potential to exceed policy limits.
- **Business interruption (BI):** Many policies only pay out for physical damage, not digital disruption. Even if cyber events are covered, waiting periods often apply, leaving firms exposed during the first few hours or days of an outage. If a cyber incident causes mechanical breakdown or non-covered perils, there is unlikely to be cover for any physical damage or business interruption losses linked to the event under a property policy.
- **Physical damage:** property policies typically only cover resulting fire or explosion, not direct physical damage caused by a cyber incident. While cyber physical risk is growing, standard property all risk policies still explicitly exclude this damage unless a specific endorsement is added, such as cyber property damage loss endorsement.

Executive views on insurance and insurers

We are seeing increasing recognition of the value of insurance policies that have risk and crisis management, and loss prevention services incorporated in them.

Statistics from the 2026/27 Risk & Resilience survey.

> **We need brokers sitting down with their clients, reviewing their cyber and property policies, and helping to identify where the gaps are to understand what kinds of products are necessary. Then working with specialty insurers like us to see how they can plug the gaps and tailor their coverage more effectively.**

Lindsay Shipper
Head of North American Commercial Property
Beazley

Case study: When regulations tighten and data rules diverge

Tighter rules, greater complexity

Firms are scrambling to keep pace as cyber and AI-related regulations tighten across the world – growing more formalised while remaining strategically, stubbornly complex.

What is emerging is a fragmented terrain: clearer expectations for preparedness, response and transparency, but a maze of divergent obligations for any organisation operating across borders.

> **Differences in how cyber risk is perceived across regions are often less about the objective threat landscape, which is global and interconnected, and more about experience, exposure, and institutional maturity. Guidance and supervisory expectations, especially in regulated sectors, now emphasise explainability, governance, data integrity, and cyber resilience, even where formal AI-specific legislation is absent.**

Nathalie David
Partner
Clyde & Co

Regulations redraw operational risk

In Europe:
Cybersecurity laws focus on enhancing digital resilience through mandatory regulations like NIS2[32] for network security, the Cyber Resilience Act[33] for hardware and software and DORA[34] for resilience in the financial sector. These laws require companies to adhere to strict incident reporting, supply chain security, and risk management if they operate in the EU.

In the United States:
The SEC's disclosure rules[35] strike with a different tempo – forcing material incidents into the open within fixed timelines and demanding annual, public accounting of a firm's cyber governance. The US CLOUD Act makes this even more difficult, as data handled by a US provider may be subject to American authority, even if the servers sit in another country, and this shapes how every decision is made[36].

The US also has heavy legislative measures including the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)[37], requiring critical sector companies to report major breaches to CISA within 72 hours, and the Computer Fraud and Abuse Act (CFAA)[38].

In the UK:
The FCA's new unified framework standardises how financial services firms report operational and third-party failures[39]. In addition, the UK's new Cyber Security and Resilience Bill[40] sets out what executives must know, how they must prepare, and what they must reveal to whom and how quickly when an incident occurs. Failure to do so is likely to end up with directors' & officers' liability (D&O) claims.

Data sovereignty

France's plan to launch a domestic video-conferencing platform, Visio, by 2027[41] is pushing firms to reconsider reliance on non-European software and platforms for sensitive communications. The issue is not quality, but control of communications infrastructure.

Video platforms now pose strategic risk. Everyday meetings generate data and institutional memory that feed AI systems, intelligence capabilities and political leverage. US providers face legal obligations that can conflict with GDPR[42] and EU sovereignty, creating jurisdictional exposure. As a result, privacy has become industrial strategy, driving efforts to keep data, and its AI value, within Europe.

> **The key lesson here is that compliance and resilience are no longer competing priorities. Firms that treat data sovereignty as a core governance issue are better positioned to meet cross-border obligations and maintain trust in an increasingly fragmented regulatory landscape.**

Ian Birdsey
Partner
Clyde & Co

Geopolitics now shapes organisations' tech stack

For years, the model was simple: US builds the tools → Europe uses them → everyone wins on efficiency. Now a new variable has entered procurement: what if access to critical software becomes political? Where the question may once have sounded paranoid, now it sounds like crucial risk management.

Navigating conflicting data regimes

Consider a global firm trying to manage its information systems; it's battling through the turbulence of being pulled in several directions at once. For one, governments are treating data as a strategic asset – asserting authority and drawing lines around where and how information is stored, processed, controlled and accessed. And so, the firm must adjust quickly even when the rules conflict. An incident that should be routine becomes harder to handle, because each jurisdiction demands something different and each one questions whether the data is being protected on its terms.

Technology choices now shape resilience

For a firm caught in the crosshairs, the message is simple. This is less about choosing one tool over another, and more about accepting that technology choices now come with political and regulatory pressure that senior leaders must factor into resilience plans. Where systems sit, which country's laws apply and whether access could be altered without warning because of changes to policy. The result is a constant effort to stay compliant while rules tighten, diverge and demand more from every system it runs.

Making complexity manageable, not minimal

The path forward lies in making complexity less cumbersome rather than pretending it can be eliminated. Resilience depends on reducing the friction between regulatory expectations, operational reality and the shifting politics of data. Firms need governance models that assume change as the norm, with structures flexible enough to absorb new rules without disrupting operations each time a jurisdiction redraws the boundaries.

Those best positioned to succeed will be the organisations that can harness the benefits of AI while demonstrating responsible design, monitoring system behaviour in real time and ensuring governance keeps pace with technological capability.

This starts with:

- **Building an integrated risk framework:** Where cyber, legal, procurement, and operations teams use a single playbook. Firms must identify their data's location, its providers and the legal regimes governing it. Then map these dependencies across cloud infrastructure, communication tools, and AI systems to anticipate jurisdictional shifts or sudden non-compliance. Clear escalation routes, documented data-flows and pre-approved response actions help the organisation act quickly even when multiple regulators are watching.

- **Implementing cross-functional governance:** Cyber, legal, procurement, and operations teams must evaluate suppliers based on sovereignty exposure alongside cost. Establishing pre-approved fallback options – such as sovereign-hosted tools or segmented architectures – prevents disruption during regulatory changes.

- **Strengthening resilience through direct communication:** Maintaining dialogue with regulators, cloud providers and strategic partners gives firms early warning of policy shifts and alternative routes when access, hosting or compliance terms change without notice.

- **Using insurance as a strategic resource:** As cross-border regulation becomes more complex, cyber insurance provides a layer of technical, legal and forensic support that helps organisations navigate incidents across multiple jurisdictions.

In a landscape defined by divergence, the advantage goes to the firms that treat resilience as a continuous discipline: mapping dependencies, anticipating jurisdictional pressure and ensuring that every system and supplier can withstand the regulatory shocks still to come.

> **"Traditional risk frameworks are no longer sufficient; boards must treat AI as a dynamic, cross-functional risk with potential impacts spanning compliance, cyber resilience, consumer protection and market integrity.**

Ian Birdsey
Partner
Clyde & Co

Methodology

About the survey

In January 2026, we partnered with research firm Opinion Matters to survey over 3,500 business leaders and insurance buyers from internationally operating companies based in the UK, US, Canada, Singapore, France, Germany, and Spain.

Participants shared their views on insurers and insurance, as well as their perceptions of risk and resilience across four key categories:

- **Geopolitical & economic risks:** Strikes, civil unrest, regulatory changes, economic uncertainty, inflation, war, and terrorism.
- **Business risks:** Supply chain instability, business interruption, boardroom risk, crime, reputation, employer liability, and ESG compliance.
- **Environmental risks:** Climate change, catastrophic events, environmental damage, emissions, pandemics, and energy transition.
- **Cyber & technology risks:** Disruption threats, technological lag, cyber security threats, and intellectual property risks.

Respondents represented a range of company sizes, from US$/CA$/SG$/GB£/EUR€ 250,000 to over 1 billion in annual revenue, across all surveyed markets.

Each country included a minimum of 50 respondents per industry sector, covering:

- Healthcare & Life Sciences
- Manufacturing, Retail, Wholesale & Food & Beverage
- Real Estate, Commercial Property & Construction
- Hospitality, Entertainment & Leisure (incl. Gaming)
- Financial Institutions & Professional Services
- Energy, Utilities, Mining, Marine & Warehousing
- Public Sector & Education
- Technology, Media & Telecoms
- Transportation, Logistics, Cargo & Aviation

The survey was conducted between 05.01.2026 and 13.01.2026.

This annual Risk & Resilience survey began in 2021 with 1,000 respondents from the UK and US. It expanded to 2,000 in 2022–2023 with the addition of Canada and Singapore, and then to 3,500 in 2024 with the inclusion of France, Germany, and Spain.

Contributors

Nathalie David
Partner
Clyde & Co

Ian Birdsey
Partner
Clyde & Co

Rory Innes
CEO and Founder
The Cyber Helpline

Ben Hobby
Partner, Baker Tilly
London

Alessandro Lezzi
Group Head
of Cyber Risk
Beazley Security

Alton Kizzier
CEO
Beazley Security

Melissa Carmichael
Head of Cyber Risks
Beazley

Francisco Donoso
Chief Product and
Technology Officer
Beazley Security

Mark Singer
Claims Focus Group
Leader, Cyber
Beazley

Raf Sanchez
Head of Global Cyber Services
Beazley Security

Wiliam Clarke
Claims Team Leader
Executive Risk
Beazley

Craig Linton
Head of US Underwriting
Management, Cyber
Beazley

Lindsay Shipper
Head of North American
Commercial Property
Beazley

References

1. Comparing AI Agents to Cybersecurity Professionals in Real-World Penetration Testing
2. Quarterly Threat Report: Fourth Quarter, 2025
3. Quarterly Threat Report: Fourth Quarter, 2025
4. 2025 Data Breach Investigations Report | Verizon
5. https://beazley.security/solutions/mxdr
6. https://beazley.security/solutions/exposure-management
7. https://www.thecyberhelpline.com/helpline-blog/2024/11/5/the-cyber-helpline-report-how-cybercrime-justice-is-failing-the-uk
8. https://assets.publishing.service.gov.uk/media/64539087faf4aa0012e132cb/Fraud_Strategy_2023.pdf
9. The Cyber Helpline
10. https://www.ncsc.gov.uk/section/advice-guidance/small-medium-sized-organisations
11. https://www.cisa.gov/audiences/small-and-medium-businesses
12. https://www.gartner.com/en/newsroom/press-releases/2025-06-25-gartner-predicts-over-40-percent-of-agentic-ai-projects-will-be-canceled-by-end-of-2027
13. What is Vibe Coding? | IBM
14. Collins - The Collins Word of the Year 2025 is...
15. LLM06:2025 Excessive Agency - OWASP Gen AI Security Project
16. What is shadow AI? Risks and solutions for businesses
17. Rise in 'Shadow AI' tools raising security concerns for UK
18. Code of Practice for the Cyber Security of AI - GOV.UK
19. Artificial Imposters—Cybercriminals Turn to AI Voice Cloning for a New Breed of Scam | McAfee Blog
20. 2026 State of the Scamiverse: The Year Scams Went Linkless
21. https://www.un.org/en/global-issues/child-and-youth-safety-online
22. https://www.unicef.org/press-releases/deepfake-abuse-is-abuse
23. https://www.mdx.ac.uk/news/2025/4/content-moderators/
24. https://assets.publishing.service.gov.uk/media/6707a9f030536cb927482f69/uk_safety_tech_sector_2024_analysis.pdf
25. https://www.ijmuk.org/techthatprotects
26. https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/part-3-guidance-on-highly-effective-age-assurance.pdf?v=395680
27. https://technologycoalition.org/resources/update-on-voluntary-detection-of-csam/
28. CrowdStrike IT outage affected 8.5 million Windows devices, Microsoft says - BBC News
29. https://tinyurl.com/4nypdnuv
30. Cyber Essentials | National Cyber Security Centre - NCSC.GOV.UK
31. https://beazley.security/insights/quarterly-threat-report-fourth-quarter-2025
32. EU Cybersecurity Strategy | Shaping Europe's digital future
33. Cyber Resilience Act | Shaping Europe's digital future
34. Digital Operational Resilience Act (DORA) - European Insurance and Occupational Pensions Authority
35. SEC.gov | Cybersecurity Disclosure
36. Criminal Division | CLOUD Act Resources
37. Federal Register : Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements
38. Justice Manual | 9-48.000 - Computer Fraud and Abuse Act | United States Department of Justice
39. https://www.moneymarketing.co.uk/news/fca-tightens-reporting-rules- as-cyber-and-third-party-risks-rise/?utm_medium=email&_hsenc=p2ANqtz--RBDNMQNsxgYJ5w_KdKuY8QQ-VNoft65cUcfkKKuOpg_J1BF1yk5y6clccBXQWx4f0xsh1SiDUDqFUaPuXvCJujwv8sJZedLVoJ024_h9Lo86OMoE&_hsmi=131391892&utm_content=131391892&utm_source=hs_email
40. Cyber Security and Resilience Bill - GOV.UK
41. https://presse.economie.gouv.fr/souverainete-numerique-letat-generalise-visio-sa-solution-de-visioconference-securisee-et-souveraine-a-destination-des-agents-publics/
42. General Data Protection Regulation (GDPR) – Legal Text

Discover more
beazley.com

Beazley plc (BEZ.L), is the parent company of specialist insurance businesses with operations in Europe, North America, Latin America, Bermuda and Asia. Beazley manages six Lloyd's syndicates and, in 2025, underwrote gross premiums worldwide of $6,100.7million. All Lloyd's syndicates are rated A+ by A.M. Best.

Beazley's underwriters in the United States focus on writing a range of specialist insurance products. In the admitted market, coverage is provided by Beazley Insurance Company, Inc., an A.M. Best A rated carrier licensed in all 50 states and its subsidiary, Beazley America Insurance Company, Inc. In the surplus lines market, coverage is provided by Beazley Excess and Surplus Insurance, Inc.

Beazley's European insurance company, Beazley Insurance dac, is regulated by the Central Bank of Ireland and is A rated by A.M. Best and A+ by Fitch.

Beazley's Bermuda entity, Beazley Bermuda Insurance Limited, is A rated by A.M. Best and regulated by the Bermuda Monetary Authority.

Beazley is a market leader in many of its chosen lines, which include Directors & Officers, Financial Lines, Cyber, Property, Marine and Aviation, Reinsurance, Accident and Life, and Political Risks and Contingency business.

For more information, please go to: www.beazley.com

BZCP151

beazley

beazley security

Beazley Security is a global cyber security firm committed to helping clients develop true cyber resilience.

Discover more at **beazley.security**

Insurance. Just different.