Book review
Inspiration for risk professionals

News & analysis
A round-up of the latest industry news and views

The interview
We catch up with Ambros Scope

cirmagazine.com

Q3/2025

CIR

CONTINUITY INSURANCE & RISK

Recall reality *No longer a rare incident, product recalls are now a structural feature of modern markets, with high-stakes risks*

Fault lines *Business interruption covers are shifting constantly to keep pace with widening gaps and changing risk dynamics*

Business Continuity Awards 2025 Winners' Review *Highlights from our annual celebration of all that is best in resilience*

The digital battleground

Structural weaknesses and under-investment leave public sector data and networks exposed

View: "The multidimensionality of emerging risks means organisations cannot treat them as marginal. They are, increasingly, at the core of strategic resilience"

The Performance of Two Dutch Flat Roof Constructions in the Event of a Fire in a PV System

Our new White Paper details fire testing of identical PV systems with two specific Dutch flat roof build-ups. It challenges the notion that flat roof insulation under PV systems should never be anything but Euroclass A1.

This research poses questions for countries other than the Netherlands.

- What would be the performance of products and configurations that are typical of other markets?
- Why is there no standardised test method for this fire scenario?
- Who will produce one, CEN or the insurance industry?

Please scan to read the full white paper.

www.kingspan.com

Kingspan®

Comment

The UK government's handling of the Covid-19 pandemic continues to damage public trust in its ability to respond to future crises, according to research published this summer, with just a small minority believing national or local systems are prepared for future emergencies. The nationwide Cabinet Office-commissioned survey of the UK population found that just 19% believed central government was ready to manage a major emergency, while only 14% felt their local authority was prepared.

Many of the 10,000 respondents to the survey explicitly cited the government's pandemic response – widely seen as slow, chaotic and poorly communicated – as the reason for their lack of trust. These findings are not surprising. Indeed, they echo last year's Covid-19 Inquiry evidence, which concluded the government had "failed its citizens" by planning for the wrong type of outbreak. Released under the banner of building resilience, this year's report instead reveals a picture of a population expecting more shocks, but lacking faith in the country's ability to manage them.

Despite widespread scepticism of government and infrastructure preparedness, the research points to a notably higher level of public trust in the emergency services. Fire, police and ambulance services were viewed far more favourably, with respondents expressing confidence in their ability to respond effectively during crises.

The importance of preparedness for low-probability events also – perhaps surprisingly, given the bulk of the report's findings – drew considerable support. Sixty-nine per cent of respondents felt that it was important to be prepared for emergencies or disasters that may be unlikely to occur, pointing to a general recognition that risk cannot be measured only by likelihood, and that HILP events still warrant attention.

While respondents revealed a broadly positive perception of the power of preparedness, they also highlight gaps in confidence and priorities. When asked whether there are effective actions people can take to prepare for emergencies or disasters, nearly three quarters agreed or strongly agreed. Just 7% dismissed the idea, suggesting that most people see value in taking at least some steps to improve readiness.

Perceptions of the extent of personal capabilities, however, revealed less confidence, with just half of respondents feeling that they could take action to prepare for emergencies that might affect their local area. In other words, while belief in the effectiveness of preparedness is high, not everyone feels equally able to translate that belief into practice. These findings suggest a clear paradigm: people endorse preparedness in principle but do not consistently act on it personally. Although nearly half of those surveyed said they had taken some personal steps to prepare – such as storing supplies or having a back-up power source – only 13% felt their household was genuinely ready for a prolonged disruption. Meanwhile, most people believe the government should lead on planning and communications, but only a small number recalled having received any advice on emergencies in the past year.

The Cabinet Office's survey results underline the hierarchy of threats as seen by the public. War stood out most starkly, although just 65% of respondents said it would have a large or very large impact on them personally if it were to affect their local area. By contrast, just over half viewed a large-scale human disease outbreak or pandemic in the same way – despite the world's recent experience of Covid-19. And roughly half felt a terrorist attack or a cyber attack on critical infrastructure would result in a large or very large personal impact – somewhat surprising given the prevalence and impact of both.

These findings highlight the gulf between professional assessments of risk and how those risks are lived and understood by the public. Outside the world of resilience, people think differently about resilience. To think of terrorism or war feels perhaps overwhelming; its consequences hard to consider. Such perceptions matter. They shape public willingness to prepare, to follow guidance, and to support wider resilience measures at a time when it is arguably needed most.

Deborah Ritchie, Editor

FUSION
RISK MANAGEMENT

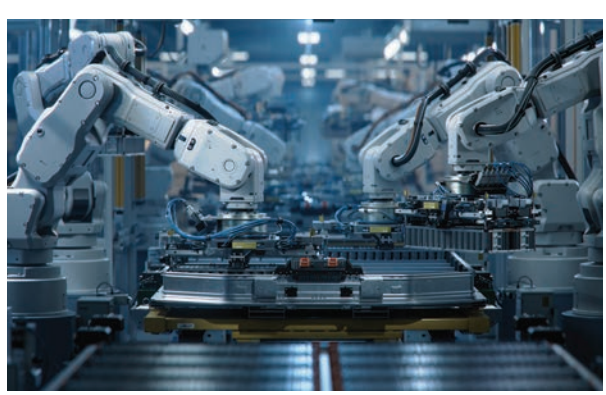
Move on from manual

BC Plan inFusion transforms static Business Continuity plans into dynamic, actionable data in minutes. Embrace the power of AI with Fusion.

G2
Leader
WINTER
2025

Visit fusionrm.com to find out more

COVER STORY



Editorial & features

News, views & regulars

CIR

CONTINUITY INSURANCE & RISK

Editorial
Deborah Ritchie
deborah.ritchie@cirmagazine.com
Tel: +44 (0)20 7562 2412

Sales
Steve Turner
steve.turner@cirmagazine.com
Tel: +44 (0)20 7562 2434

Production
Matt Mills
matt.mills@cirmagazine.com
Tel: +44 (0)20 7562 2406

Publishing director
Mark Evans
Tel: +44 (0)20 7562 2418

Managing director
John Woods
Tel: +44 (0)20 7562 2421

Subscriptions
To subscribe, please complete our registration form online at www.cirmagazine.com

CIR Magazine is published by:

Perspective Publishing Ltd
5 Maidstone Buildings Mews
London
SE1 1GN
England

ISSN 1479-862X
cirmagazine.com

THE NATURAL CHOICE TO BETTER MANAGING RISK AND UNCERTAINTY

For over 20 years riskHive have delivered innovative software solutions supported by Subject Matter Expert training and consulting that helps organisations to better manage risk and uncertainty, delivering improved confidence to stakeholders.

Risk and Opportunity Management.

Business Continuity and Resilience.

Cost Assurance and Forecasting.

riskHive®

riskHive Software Solutions Ltd
United Kingdom, BS48 4PG
+44 (0)1275 545874
info@riskhive.com
www.riskhive.com

AI adoption outpaces efforts to ensure security

Shadow AI and ungoverned artificial intelligence are emerging as major drivers of costly data breaches, according to a new report, which shows organisations adopting AI faster than they can secure or oversee it

Artificial intelligence is transforming the way organisations approach cyber security – but the pace of adoption is outstripping the development of governance frameworks, according to a new report from IBM. It found that companies are deploying AI quickly to drive efficiency, accelerate detection and enhance breach response, at the cost of significant risks.

IBM's 2025 *Cost of a Data Breach Report* provides detailed insights into these emerging risks. Based on research covering 600 organisations across 17 industries in 16 countries, the findings show that AI adoption is currently outpacing governance – with 97% of AI-related breaches involving systems that lacked proper access controls. Furthermore, 63% of organisations either do not have an AI governance policy or are still developing one. Even among those with policies, less than half have an approval process for AI deployments, and 61% lack governance technologies. Only 34% of organisations perform regular audits for unsanctioned AI use, leaving many AI systems unchecked.

Shadow AI, defined as the use of AI tools without formal approval or oversight, has emerged as a major vulnerability, allowing unmonitored systems to expose sensitive data and create compliance gaps. Attackers are also exploiting AI, using generative tools to scale phishing campaigns and deepfake impersonations – making AI both a defensive and offensive tool in today's cyber landscape.

The financial impact of these gaps is already evident. Shadow AI contributed to 20% of breaches in the study, adding an average of £529,000 to the breach cost for organisations with high levels of unmonitored AI. These incidents often affected multiple data types simultaneously, with 65% of breaches compromising personal identifiable information, and 40% involving intellectual property. The data was frequently stored across multiple environments, demonstrating that even a single ungoverned AI system can have widespread repercussions.

Despite the risks, AI is also providing measurable benefits in breach response. Organisations using AI and automation extensively across the security lifecycle – including prevention, detection, investigation and response – shortened breach resolution times by 80 days, and reduced average costs by £1.5m per incident. Nearly a third of organisations reported extensive use of these tools, although the majority remain underused, indicating that the cost benefits of AI have not yet been fully realised.

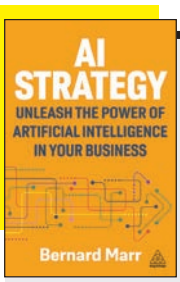
Breach costs

Overall, breach costs show a mixed picture. The global average dropped to £3.5m in 2025, a nine per cent decline from 2024, largely driven by faster breach containment aided by AI. The United States represents an outlier here, with average breach costs surging past £8m due to higher regulatory fines and detection costs. Threat vectors have also evolved – phishing remains the most common initial attack type at 16% of breaches, averaging £3.79m per incident, while malicious insider attacks remain the costliest, averaging £3.88 million per breach. Third-party vendor and supply chain compromises follow closely, reflecting the expanded attack surface organisations face today.

AI-driven attacks are increasingly part of this landscape. The report shows that one in six breaches involved attackers using AI, predominantly for AI-generated phishing emails or deepfake impersonation. Generative AI has drastically reduced the time required to craft convincing phishing content, from 16 hours down to five minutes, amplifying the scale and sophistication of attacks. As a result, organisations are facing a cyber security arms race.

IBM's latest report emphasises that governance is now a critical factor in managing AI risk. Organisations cannot rely on adoption alone; structured oversight, access controls and auditing are essential to prevent unmonitored AI systems from becoming costly vulnerabilities, with the combination of shadow AI, insufficient governance, and evolving attack methods underscoring the importance of integrating security and operational controls at every stage of AI deployment.

Inspiration for resilience professionals



AI Strategy: Unleash the Power of Artificial Intelligence in your Business

Bernard Marr
Kogan Page, 2025
koganpage.com

Artificial intelligence is the single greatest groundbreaking force in business today – driving productivity change, and accelerating advances in other technologies along the way. "It is," as author Bernard Marr writes, "without doubt, the great breakthrough technology of our times" – and like fire, steam power, electricity and computing before it, AI will continue advancing. "There's no putting the genie back in the bottle," the author notes. "AI is here to stay. And your business had better get ready for it."

A futurist and thought leader in the fields of business and technology, Marr has a passion for using technology for the good of humanity. A best-selling author of over 20 books, Marr is committed to exploring and sharing ideas that can help create a better future through responsible AI adoption, and counts some of the world's best-known brands among his clients – from Amazon, Cisco and NVIDIA to Shell, Toyota and Walmart.

In his latest book, Marr writes that AI is forecast to add more than £11.6 trillion to the global economy by 2030, and to deliver a 26% boost in GDP in local economies. (Generative AI alone could add up to £3.4 trillion a year to the global economy – more than the UK's entire GDP in 2021.) "What business can afford to ignore such a transformative technology?" Marr rightly asks.

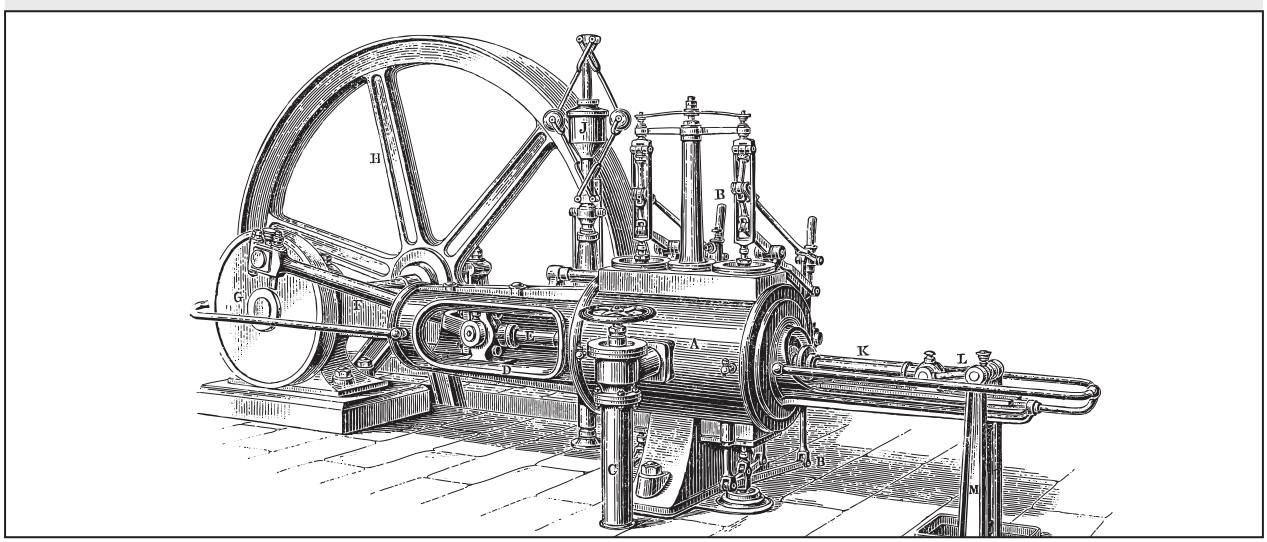
At the same time, AI is poised to revolutionise the way we work, affecting almost 40% of jobs around the world. In advanced economies, that figure could be as high as 60%. "Some jobs will be replaced by AI-led automation, some jobs will change, and new jobs will emerge – just as with previous breakthrough technologies," the author writes.

Despite AI's staggering promise, and its potential future impact on the workforce, a third of managers in the UK have never used AI. That being the case, how can business leaders imagine what can be done with AI if they've never used it, he asks?

It's not too late for business leaders to get on board, Marr says. Although AI – especially Gen AI – has been a buzzword for a couple of years, it's still very much early days in its transformative impact, making now the perfect time for business leaders to get to grips with it.

Drawing on the author's interactions with the business leaders, technologists and practitioners that are shaping AI's future, *AI Strategy* covers every aspect of AI adoption – from ethics to upskilling, and data management to tech infrastructure. In addressing all these impacts, the book uses real-world examples across multiple organisations and industries – from energy, healthcare and education to marketing and HR.

Wherever you are on your AI journey, this essential guide will help you craft and execute a strategy that has the potential to create meaningful impact – hopefully both within and beyond your own organisation.



Steam power: A breakthrough technology in its own time

News briefing

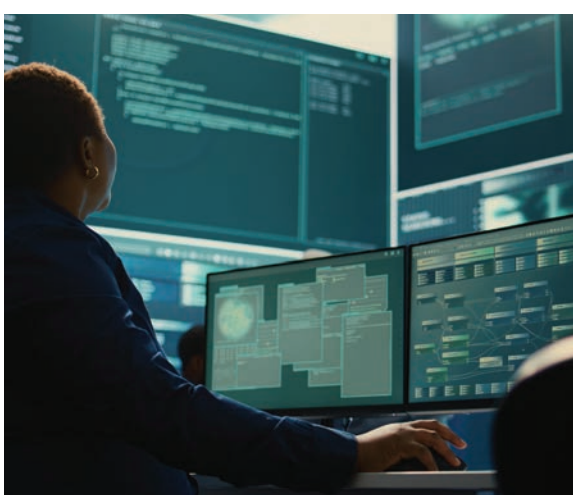
A round-up of the latest industry news

Escalating political polarisation was found to be associated with increased political violence and unpredictable oscillations in government policies, according to the latest *Political Risk Index* from Willis. Countries enduring violent political conflicts tend to be the most polarised it said. On average, affective polarisation is rising fastest in the US, Germany, India, Brazil and Bulgaria.

The UK Government's handling of the Covid-19 pandemic continues to damage public trust in its ability to respond to future crises, new research suggests – with only a small minority believing national or local systems are prepared for future emergencies.

Confidence seems in short supply elsewhere, as UK firms reportedly lack trust in third-party vendors to manage critical risks. Nearly three in ten UK organisations do not trust their third-party vendors to manage critical risks, according to research conducted by cyber consultancy CyXcel. The findings suggest firms are outsourcing high-stakes responsibilities without the internal visibility needed to assess vendor capability.

The Financial Conduct Authority fined Barclays Bank UK plc and Barclays Bank plc a combined £42m for failings in financial crime risk management involving WealthTek and Stunt and Co.



The FCA fined Monzo Bank Ltd over £21m for inadequate anti-financial crime systems and controls between 2018 and 2020. The bank also repeatedly breached a requirement preventing it from opening accounts for high-risk customers between 2020 and 2022, the watchdog said.

HMRC admitted that £47m was stolen through a phishing-driven breach affecting thousands of PAYE tax accounts. The incident emerged inadvertently during a House of Commons Treasury Select Committee hearing on the department's struggling performance, sparking further scrutiny of its management and oversight.

The Cyber Monitoring Centre categorised the disruption to retailers M&S and Co-op following the April 2025 cyber incident as a Category 2 systemic event. In its first live public assessment of a cyber incident's financial impact in the UK, the CMC calculated that the cost of the ransomware attack on the two retailers and associated parties would fall somewhere between £270m and £440m.

Four people were arrested in the UK as part of the National Crime Agency investigation into the cyber attacks targeting M&S, Co-op and Harrods. Two men aged 19, another aged 17, and a 20-year-old woman were apprehended in the West Midlands and London on suspicion of Computer Misuse Act offences, blackmail, money laundering and participating in the activities of an organised crime group.

Workplace deaths have fallen to pre-pandemic levels, according to the latest figures from the Health and Safety Executive. The figures show that 124 workers were killed in work-related incidents in Great Britain in the year to March 2025 – a decrease of fourteen from the previous 12-month period. This compares with 223 deaths twenty years ago (2004/05) and 495 in 1981.

For the full story behind all these headlines, visit **cirmagazine.com**

Finance professionals expect employers to reduce their focus on sustainability and diversity commitments moving forward. This was amongst the findings of research carried out by credit information provider, CRIF. The findings draw upon the views of financial services professionals from the UK and Europe.

Cyber events that cause reputation risks can lead to a 27% drop in shareholder value, according to analysis from Aon. The findings build on 2023 research that found major cyber incidents led to an average 9% decline in shareholder value over the following year.

Insurers identified geopolitical instability as the greatest threat to the aviation sector, according to a new survey. Two-thirds of respondents working for international aviation re/insurers put the impact of war and international conflicts at the top of their list of concerns. Their views were sought as part of research conducted by the International Union of Aerospace Insurers' Cyber and Emerging Risks Study Group.

Meanwhile, less than a third of senior aviation executives believe their business strategies are equipped to meet the emerging risk challenges of the next ten years, according to a new study conducted by Willis.

Separately, the International Underwriting Association called for legal reforms to support the safe development and insurance of emerging aviation technologies including air taxis and drone deliveries. Responding to a Law Commission review of autonomous flight law, it said insurers are already beginning to offer innovative cover for unmanned systems but need stronger legal foundations to help them assess and price risk more accurately.

The FCA raised concerns that some insurers may be profiting excessively from premium finance, as it continues its investigation into whether customers paying monthly for insurance are receiving fair value.

The UK Government announced its long awaited plans for a new UK captive insurance regime, in a major policy shift intended to help the UK compete with established captive domiciles. The new regime is expected to introduce a light-touch regulatory framework, supporting the formation of captive insurers onshore, and encouraging existing captives to relocate to the UK.

Cumulative fines under the General Data Protection Regulation surpassed £5.3bn by the end of May, eight years after the EU's landmark regulation came into force. Ireland tops the table for total value, with over £3.4bn in fines, while Spain leads on volume, recording 958 penalties.

An increase in the number of extreme heat events counts amongst the most significant emerging risks, according to research published by Swiss Re. Its latest SONAR report points to longer, hotter heatwaves and their increasing cost to human life and infrastructure.

The FCA confirmed that bullying and harassment will qualify as misconduct across a wider section of financial services. The watchdog issued draft guidance to help firms assess non-financial misconduct when determining whether an individual is fit and proper to work in financial services. This includes behaviour in personal life.

Leadership in the digital era

Deborah Ritchie speaks to Zurich Insurance's head of leadership and future of work, Ambros Scope, about leadership, post-pandemic workforce challenges, and the importance and power of harnessing artificial intelligence in the right ways

How have recent societal and technological developments impacted the role of human resources in the insurance industry?
One of the key changes is that HR has shifted from being an operational to a more strategic function. Let's look at leadership: they say that people join a company because of the company, but leave because of their boss. This serves to underline how important leadership and cooperation skills are in any organisation. Despite all the technological changes that we're seeing, we're still human beings working with each other.

"Despite technological change, we're still human beings working with each other"

Think about the both the best and worst managers you've ever had. The level of motivation sparked by these two people is worlds apart, right? Multiply that by employee numbers, and you begin to see the large-scale impact of leadership on business results. A modern HR department aims to improve these aspects – leadership, cooperation and motivation. It's no longer just about hiring, administration and payroll. That's not how I see HR, and not how we run leadership development at Zurich.

What does positive leadership look like in practice in a post-pandemic working environment?
Positive leadership is about respecting others as humans, understanding what they're interested in, what they want to learn, and how they can show the best version of themselves. It's not about commanding someone to do something by Monday, and then criticising the output without appreciation. That kind of micromanaging leadership is old-school, and thankfully becoming much less common these days.

Scope: Adaptability is the cornerstone of effective leadership amid change

During the pandemic, I think managers saw that people remained motivated and productive without constant oversight. That helped us move away from micromanagement. Yes, some people weren't as self-directed, but that becomes obvious before long, and can be managed.

Should artificial intelligence be used to help address this challenge?
We want to avoid that kind of use of AI. There are strict regulations – especially in Europe – around AI profiling and decision-making without human supervision. AI cannot and should not make important decisions about employees on its own. What's missing in machines is consciousness. You never quite know what the machine will decide and, without supervision, AI can evolve in directions you don't want – social media already offers numerous examples of that. Oversight is essential. AI should support human decisions, not replace them.

How do you see AI being deployed to support a more productive workforce in a way that respects vital regulatory and ethical boundaries?
AI in its basic form has been around for years but GenAI has made the available tools much more visible to more people, which creates the impression of a sudden shift. In reality, AI's development has unfolded in waves – periods of intense hype followed by deep disappointment (often referred to as an 'AI winter') when the technology failed to meet expectations.

The key is separating personal and operational efficiency. ChatGPT, for instance, is excellent for speeding up certain tasks. But for an insurance claims department, say, with thousands of claims being reported every day, and thousands of different customer journeys, then GenAI is not as helpful as you might think. You still have to deal with your processes and your systems, and that demands something more structured.

We're running leadership programmes that build AI and intelligent automation skills. We say to our leaders: ChatGPT is great, but the real return on investment comes after you've clarified your processes. First, optimise your processes and systems – then layer AI on top. Only then can you see true gains.

"In the near future, even video meetings won't guarantee that you're talking to a real person. We may need new ways to confirm human identity"

Even in a company like Zurich, which is very advanced in its use of AI, we recognise that it only works if your systems and processes are ready. You can't go cross-country in a race car – you need a flat, clear track. Then the race car helps!

Smaller companies and start-ups without legacy systems can obviously be more nimble in this respect – in the same way as how some developing countries leapfrogged landline infrastructure and went straight to mobile – and now use mobile payments more efficiently than some parts of Europe.

Large, established companies can't just throw out their systems and start fresh. They have to build in AI carefully, step by step.

Could digital twin avatars soon replace humans in meetings? Was Mark Zuckerberg correct in forecasting this shift?
Currently I don't see a widespread use of digital twin avatars but we've already seen instances, like the high-profile case in Hong Kong, where a fake CEO avatar succeeded in convincing an employee to transfer millions to a bogus bank account. Even at a smaller scale – like someone's child receiving costly premium text messages – these threats are real today.

Because of these developments, human interaction becomes even more valuable. You and I could have conducted a conversation over email, but would we have connected the same way? In the near future, even video meetings won't guarantee that you're talking to a real, or specific, person. We may need new ways – codes or systems – to confirm human identity. That could be a technical solution that works in the background, or asking for personal information that an avatar would not know.

Cyber risk isn't a future problem. It's happening now, every day, in different forms. That's why we also use AI to monitor our systems for suspicious activity.

Given your background in mechanical engineering, how do you see systems thinking being applied to leadership and workforce planning?
Systems thinking, to me, starts with end-to-end thinking. Some start-ups build solutions first, then look for problems – which is a backwards approach. We should start with the problem and then develop a solution. And before bringing in AI, you need to sort out your processes and systems. Only then should you layer in AI to accelerate and improve them.

There's also a human side. Systems thinkers often want everything to be neat and predictable. Today, you have to be comfortable with ambiguity. Agile thinking – starting with prototypes and improving them over time – is key.

Interview by Deborah Ritchie

The digital battleground

The recent Ministry of Defence data breach highlights persistent vulnerabilities in public sector data security efforts, while unrelenting ransomware and AI-driven attacks reveal structural weaknesses in wider cyber resilience

The digital battlefield is shifting quickly, and government services risk falling behind as attackers exploit every gap in their defences, leaving vital services exposed and data at risk. Human error, under-investment and structural weaknesses make public bodies low-hanging fruit for criminal groups and hostile states, whose toolkits are advancing rapidly, with artificial intelligence-powered attacks an increasing concern for organisations already struggling on a daily basis to keep pace with more traditional digital risks.

Ransomware is among the top threats. The high-profile 2024 attack on Synnovis, a pathology laboratory processing blood tests, led to the theft of patient data and severe operational disruption, contributing to at least one patient death due to delays in testing. Ransomware has disrupted local council services – from social care and waste collection, and schools were this year unable to process GCSE and A Level coursework as a result of attacks made during these critical periods.

The HMRC phishing scam in 2025 exposed a different kind of digital risk, resulting in £47 million being stolen when organised groups used stolen identity data from outside HMRC systems to impersonate taxpayers and manipulate accounts. While HMRC's core systems were not breached, the incident revealed critical vulnerabilities in identity verification and fraud controls, highlighting an urgent need for enhanced digital risk management and security measures.

"It feels like cyber risk is accelerating away from public sector organisations' ability to keep up," says Chris Butler, resilience director at Databarracks, which provides managed services including data back-up, disaster recovery and business continuity planning.

He notes an increasing level of engagement among senior leaders in the sector as they grapple with the threats.

"There's an ever-greater realisation [of] these risks and the need to minimise the disruption they can cause," he says. "That means looking at people and processes and running complex simulations."

The unique structural and procedural challenges faced by public sector organisations make cyber security a tough risk to grapple with.

"Public sector organisations present themselves as low-hanging fruit: they have lots of data and in many cases there has been under-investment in their cyber security capabilities"

Alistair Clarke, UK cyber broking leader at Aon, whose team places cyber insurance and reinsurance for public sector organisations, cautions that bureaucracy can slow response and inhibit joined-up network security strategies. Leadership turnover following elections disrupts strategic planning and continuity, while resource constraints leave many organisations underprepared.

"Those structural issues, as well as a lack of funding, can make all of this really difficult," Clarke says. "I'm sure they're doing everything that they feel they can, but there are reasons why some organisations are more at risk than others."

Clarke also highlights the dangers posed by new AI-powered threats.

"They are finding ways to reach people at senior levels within organisations and present themselves as part of the organisation requesting funds," he explains. "The technology is moving so quickly."

Clarke also points to traditional cyber risks, particularly those caused by human error.

"You can risk manage some of that, but it's difficult," he says. "Human error and a lack of awareness are set against evolving cyber threats. Unfortunately, public sector organisations present themselves as low-hanging fruit: they have lots of data and in many cases there has been under-investment in their cyber security capabilities."

Endemic data security issues

Device security remains a stubborn issue, with multiple departments reporting increases in lost or stolen equipment despite audits and mitigation efforts. Freedom of Information requests submitted by Apricorn earlier this year show more than 1,200 organisational devices lost

or stolen across 17 departments in 2024, with HMRC alone accounting for 804, including 499 mobile phones – adding to mounting evidence of systemic security weaknesses at the tax authority. Many losses arose during audits of legacy equipment, exposing ongoing inventory management challenges. The House of Commons reported 100 devices lost or stolen, up from 65 the previous year. The Department for Education saw device losses climb from 78 in 2023 to 107 in 2024. The Department for Energy Security and Net Zero also reported an increase, from 122 lost devices in 2023 to 150 in 2024, while the Department for Science, Innovation and Technology disclosed 113 missing devices.

Apricorn's FOI request also revealed continuing personal data breaches. The House of Commons reported 49 incidents in 2024, up from 41 the previous year. Both the Ministry of Justice and DfE refused to disclose breaches or reports made to the Information Commissioner's Office, citing exemptions under Section 24(2) of the FOI Act.

The most recent high-profile incident to underscore the potential fallout from data security missteps came to light in July 2025, when a Ministry of Defence data breach from February 2022 was uncovered. An MoD official mistakenly emailed a spreadsheet containing personal details of around 18,700 Afghan applicants and their families. The breach was kept secret under a super-injunction until July 2025.
As a result, about 6,900 at-risk Afghans were secretly resettled under the Afghanistan Response Route, costing up to £850 million amid efforts to protect them from Taliban reprisals.

Improvement efforts

Despite all these incidents – and no doubt a number of un- or under-reported cases besides – efforts to combat these incidents abound, with initiatives launched by both the current and previous governments in an effort to stem the tide.

As the UK's technical authority for cyber threats, and part of GCHQ, the National Cyber Security Centre monitors cyber incidents, provides early warnings, threat assessments, guidance and support to both the public and private sectors. The NCSC is the single point of contact for cyber incidents under UK and EU regulations, coordinating responses and cooperation nationally and internationally to mitigate cyber risks and protect critical infrastructure.

"We identify vulnerabilities, share threat intelligence, provide practical advice, and help organisations prepare

for and respond to incidents," says Jonathon Ellison, director for national resilience at the National Cyber Security Centre. Its Early Warning Service flags emerging threats, while the Cyber Assessment Framework provides guidance for managing cyber risks.

The National Audit Office, meanwhile, has published a Good Practice Guide for managing risks in government. Recommendations include establishing a strong leadership and risk culture, building capability and expertise while knowing when to bring in external assistance, and enabling "interdependent and interconnected risks to be identified and managed in a robust and integrated manner."

Elsewhere, both the National Cyber Security Council and the Local Government Association have produced guidance, training and resources to help organisations understand risks and improve cyber resilience. And in July 2025, the government announced new measures designed to protect the sector against ransomware attacks, by officially banning payment of ransomware demands and introducing a mandatory reporting regime to help identify perpetrators.

Emphasising the need for a cultural shift, Ellison says cyber security should not be reduced to being seen as a cost, barrier or compliance issue, but framed as a "critical enabler for success".

"As in other aspects of managing and delivering public services, sometimes an investment really can deliver much greater value than a cut," he adds.

Local government

For local government specifically, the Ministry of Housing, Communities and Local Government runs a Cyber Support programme for local councils, a capability still conspicuously absent.

"Local councils have struggled with under-investment," Clarke says, pointing to the persistent reluctance of councils and authorities to buy cyber insurance.

A separate FOI request by Apricorn underlines the scale of the gap. Of 41 local councils questioned, only two had a cyber insurance policy in place. The majority either declined to respond, confirmed they had no cover, or made clear they had no intention of investing in it. Suffolk County Council, which disclosed 334 breaches in the same request, said it manages cyber risk in-house.

This lack of cover exposes a structural weakness. Speaking at the British Insurance Brokers' Association Conference in Manchester earlier this year, NCSC chief executive, Lindy Cameron, stressed that cyber insurance remains one of the few market-based levers for driving organisations to adopt stronger security controls and resilience measures. She said the sector could be a "force for good in making the UK the safest country in the world to do business".

The catalogue of breaches and disruptions shows that when it comes to digital risk, the stakes are higher than ever for public sector organisations. These are the systems that keep the country running and protect its most sensitive data, underscoring the urgent need for stronger security, better leadership and a culture that takes resilience seriously.

Public sector ransom payments outlawed

The UK government is taking a bold step in the fight against ransomware by outlawing ransom payments from public sector bodies and operators of critical national infrastructure. The ban, the proposals for which were announced in July 2025, applies to organisations such as the NHS, local councils, education providers and utilities companies.

The move follows a lengthy public consultation, and represents a clear shift in how the UK approaches one of the most pervasive forms of organised cyber crime. Until now, ransom payments were not explicitly prohibited under English law unless they involved terrorist financing. The new regime not only prohibits payments across the public sector, but also requires private sector organisations to notify the government if they intend to meet a ransom demand.

For policymakers, the aim is twofold: to choke off the illicit economy that rewards attackers, and to increase the transparency and intelligence around how, when and why organisations are targeted. Ministers argue that by outlawing payouts in the parts of the economy that deliver essential services, they are removing one of the central incentives that drive ransomware operations.

The ban is expected to have far-reaching consequences for the insurance market. London has traditionally been the global home for specialist kidnap and ransom cover, and cyber policies have often offered assistance that, in practice, could help clients negotiate or even meet ransom demands. Now, those products face a period of re-examination. With the new legal baseline in place, insurers will come under pressure to tighten underwriting and, in some cases, reconsider entire product lines.

Separately, the Information Commissioner's Office has made clear that payment does not mitigate the regulator's response – data protection fines or enforcement action can still follow.

The reform crystallises an expectation that paying a ransom should not be seen as an acceptable fallback. Already, many organisations have begun to improve their recovery posture – strengthening back-up regimes, stress-testing continuity plans, and rehearsing incident response, according to data compiled by Databarracks.

The government hopes that the sector-wide ban will accelerate those much-needed cultural and operational shifts, forcing bodies that perform critical public functions to harden resilience.

airmic

JOIN US.

Driving transformation in risk and insurance.

www.airmic.com

Take a free membership test drive and see what we have to offer.

Airmic Ltd, Marlow House, 1a Lloyd's Avenue, London EC3N 3AA

If you want peace, prepare for war

In his new book *The Russia-Ukraine War – Security Lessons*, Dr Simon Bennett analyses the conflict with a view to drawing lessons that, if actioned, could help the West prepare for a wider European or world war

The collapse of the Soviet Union affected KGB officer Vladimir Vladimirovich Putin profoundly. Determined to restore the Russian empire, Putin fought his way to the top of Russia's political tree. Putin always considered Ukraine a part of Russia.

In 1994, Boris Yeltsin, along with US President Bill Clinton and British Prime Minister John Major, signed the Budapest Memorandum on Security Assurances. The Memorandum guaranteed Ukraine's borders.

Putin, determined to restore Ukraine to Moscow's orbit, had no intention of honouring the 1994 Memorandum. In 2014, he walked into Crimea. In 2022 he attempted to take Kyiv. Following Putin's annexation of Crimea, the West could have stationed troops in Ukraine to deter further aggression. Misreading Putin, the West chose appeasement over action, a cowardly decision that has cost Ukraine dear.

The more diversified and distributed a country's power generation system, the more resilient it is

Lessons from the conflict

The Russia-Ukraine war holds important lessons that, if actioned, could help European states survive a confrontation with Russia. In my new book *The Russia-Ukraine War – Security Lessons*, I describe what I consider to be the most important lessons from the conflict, a number of which I outline here.

Since the collapse of the Soviet Union, across Europe, factories, laboratories, research and development facilities, power stations, transportation hubs, medical facilities and all the other elements of a modern economy have been sited and fabricated with little thought for how they might fare in time of war when, as the Russia-Ukraine conflict has shown, they may be targeted with glide-bombs, drones, cruise missiles and ballistic missiles – supersonic and hypersonic. In their decision-making, European politicians, industrialists, financiers, shareholders and planners have created manufacturing capacity that is efficient rather than resilient – fine for peace-time, but a hostage to fortune in wartime. The Russia-Ukraine war has demonstrated the need to protect critical national infrastructure and manufacturing capacity through layered air defence, electronic warfare, hardening, dynamic camouflage techniques and dispersal. Hardening might involve moving production facilities underground (as Britain and Germany did during the Second World War). Dispersal involves scattering the elements of a production facility across as large an area as possible, reducing the chances of an air barrage triggering a chain reaction. Dispersed – loosely coupled – production facilities are more resilient than concentrated – tightly coupled – production facilities.

Grangemouth oil refinery complex, on the Firth of Forth in Scotland, is one of the largest of its kind

Production facilities must be preserved. Instead of allowing loss-making plant like steelworks and oil refineries to be decommissioned by self-interested company boards, financiers and shareholders, such plant should be purchased by governments and mothballed, ready to be reactivated in time of war. Military planners forecast a major European war in five to ten years. In light of such forecasts, the closure of, for example, Scotland's Grangemouth oil refinery in April 2025 and the planned closure of Immingham's Lindsey Oil Refinery are inexplicable and dangerous. Successive governments have failed to grasp the need to preserve every component of Britain's industrial base. Britain's political class is myopic – the country's industrial base is threatened by extortionate energy costs, attributable in part to green taxes. Given that nothing the UK does will slow global warming, why destroy industries that will be essential in time of war? Surveying the Grangemouth closure, *The Sunday Telegraph* journalist Jonathan Leake noted on 17th August: "Bosses at… Grangemouth…said last week it had not made a profit for five years because of the taxes and levies imposed on the gas it consumes". Britain's green taxes, pushed by Keir Starmer's secretary of state for energy, are a gift to the Kremlin. In security terms, they are a latent error or resident pathogen – a disaster waiting to happen.

A national power generation system built around a small number of monolithic power generation units – for example, large nuclear power stations – is less resilient in time of war than a national power generation system built around a large number of small power generation units – for example, neighbourhood waste-to-power stations, community wind and solar farms, civic hydro-electric schemes and tidal barrages, compact coal, gas, oil, wood and peat-burning power stations and mobile petrol and diesel-powered generators. The more granular, diversified and distributed a country's power generation system, the more resilient it is.

As demonstrated by Ukraine's innovative drone manufacturing sector, a strong indigenous defence industrial base, supported by relevant university teaching and research, is a prerequisite for success on the battlefield. America's military-industrial complex, a product of the Second World War, has kept it the world's preeminent military and political power for nearly eight decades. Author Erin Morgenstern wrote: "All empires fall, eventually". Despite setbacks such as the 1975 loss of South Vietnam, the 1979 Iranian hostage crisis, and the 2001 terror attacks on the US mainland, *Pax Americana* endures, much to the chagrin of America's enemies.

Globalisation

In time of war, the inter-state dependencies created by globalisation render participating states vulnerable. While globalisation delivers economic benefits under peacetime conditions – with, for example, states able to source the cheapest components – under wartime conditions, trading partners may be unable or, because their loyalties lie elsewhere, unwilling to supply essential matériel. Under these conditions a country's advanced weapons systems may be rendered unserviceable – expensive junk fit only for recycling. Like his predecessor, Trump is resolved to re-shore essential industries such as microchip manufacture.

In the matter of military procurement, technophilia – an obsession with high-technology weapons systems – is a dysfunction. While advanced systems have their uses, so too do cheap, simple to use systems that can be produced at volume by semi or unskilled workers in improvised factories and quickly deployed to the front-line. The simple drones used by Ukrainian troops during the early stages of the war to gather intelligence and attack troops and soft-skinned vehicles are a case

in point. History holds lessons for arms procurers. During its time in Vietnam, the US Army created a South Vietnamese army in its own image, that is, a force built around advanced weaponry. Unfortunately for the Army of the Republic of Vietnam – at one time the fifth largest army on the planet – when the US withdrew from South Vietnam it reduced, then halted its maintenance support for the ARVN's advanced weaponry. The ARVN imploded and South Vietnam was lost to the communists.

States are wont to abandon allies or change sides out of self-interest. In 1972, US President Richard Nixon promised South Vietnamese President Nguyen Van Thiêu air support (in the form of B52 Arclight carpet bombing missions) should his country find itself under threat from the North Vietnamese Army and Viet Cong. Nixon's security guarantees proved worthless. Despite NVA and VC insurgencies, Nixon, determined to improve his poll ratings by extricating the US from the Vietnam quagmire, withheld the promised air support. Thiêu felt betrayed. Although some ARVN units mounted an heroic defence, on 30th April 1975 the NVA and VC walked into Saigon. In August 2025, Trump, who, during the 2024 presidential election campaign, had promised to end the Russia-Ukraine war, applauded Putin as he strutted down a red carpet in Alaska. History teaches that, in a perfidious world, treaties and security guarantees are largely worthless. Security issues from self-reliance. It issues from the barrel of a gun.

The West's refusal to deploy troops to Ukraine following Putin's annexation of Crimea was likely read by him as an invitation to attack Kyiv. Had Western nations used strategic empathy – a foundational tool of statecraft – to gameplay how Putin might read (perceive) the West's surrender over Crimea, it is possible they would have dispatched troops to Ukraine to deter further aggression. Had this been done, today's bloody quagmire might have been averted.

Military mindfulness – a capacity for creative thinking – is a force multiplier. Witness how the Ukrainian military's revival of Jagdkampf – the doctrine of irregular warfare centred on small, mobile and autonomous fighting units – helped the army repel Russia's 2022 assault on Kyiv.

Actioning lessons learned

If we understand the Cold War as an ideological conflict between authoritarianism and liberalism, then it did not end with the collapse of the Soviet Union. The ideological conflict that fuelled the Cold War continues. In light of serial warnings of armed conflict – for example, Russia's invasion of Georgia and conquest of Chechnya – Western disarmament seems, in hindsight, naïve, if not suicidal.

Europe will only survive if it stops talking about security guarantees – which, in the context of Putin's duplicitous and colonialist regime and US President Donald Trump's isolationism, are worthless – and rearms at pace. In 1938 in Munich, Hitler stated in writing he had no unmet territorial ambitions. In 1939 he walked into Czechoslovakia. In 1994, Yeltsin signed the Budapest Memorandum. In 2014 Putin walked into Crimea. Weapons and the will to use them are the only effective security guarantees. Appeasement never works.

In my book I talk about the importance of actioning lessons learned, that is, of active learning. Churchill understood the importance of active learning. "Those who fail to learn from history are doomed to repeat it" he warned. If we want peace we must prepare for war. That is the realpolitik of today's dangerous world. In June 2025, Britain's Labour Government published its Industrial Strategy. An industrial strategy that lets strategic assets such as oil refineries, steelworks and chemical plants go to the wall is, in the context of the threat posed by Putin's Russia, not worth the paper it is written on.

About the author

Dr Simon Ashley Bennett is an expert in the field of risk management, particularly as it relates to commercial and military aviation safety. He is known for his expertise in Crew Resource Management, a team-building methodology that has significantly improved aviation safety. He has hands-on experience working on aircraft flight decks, consulting for companies including easyJet and DHL Air, and has supervised PhD research on reducing friendly fire incidents in NATO operations and comparing teamworking in healthcare and aviation.

Bennett's research focuses on the organisational, social, economic and political origins of risk, including issues like groupthink, corruption, political instability, terrorism and armed conflict. He is involved in the Air Safety Group of the Parliamentary Advisory Council for Transport Safety and has authored books on aviation safety and the weaponisation of nuclear facilities during conflict.

His academic background includes a PhD in the sociology of scientific knowledge. He is respected for combining practical industry experience with sociological and risk theory perspectives.

Dr Simon Ashley Bennett is director of the Civil Safety and Security Unit at the University of Leicester

***The Russia-Ukraine War – Security Lessons: An Analysis Informed by Sociological Approaches to Risk Management* is published by Peter Lang International Academic Publishers**

CIR Software Reports

CIR's fully interactive online software comparison tool is available across all our reports, in addition to our popular in-depth analysis of products in the business continuity, emergency and mass notification, and risk software markets.

Visit cirmagazine.com

Recall reality

In global markets, product recalls have evolved from rare incidents to recurring, high-stakes risks. As a result, manufacturers and insurers face mounting regulatory, operational and reputational pressures, with recalls now a structural feature of modern markets

In an era of complex global supply chains and heightened regulatory scrutiny, product recalls are one of the most acute and costly risks facing manufacturers and their insurers. Recalls are no longer rare crises but structural features of markets under intense legal, consumer and reputational pressure. The implications stretch well beyond the immediate logistics of retrieval into brand value, litigation exposure and insurability.

The current poster child for product recall is the Takata airbag. The global airbag recall, which began in 2013, affected around 100 million vehicles, caused at least 30 deaths, hundreds of injuries, imposed total costs on the company and automakers of around £18.5 billion, and led to the bankruptcy of Takata.

More recently, Tesla's divisive Cybertruck SUV has been recalled eight times since its December 2023 launch, for defects ranging from incorrect font size on dashboard warnings to unintended acceleration from a trapped pedal. The cases illustrate the spectrum of safety issues – from weak pre-launch testing to potentially lethal outcomes – and the regulatory and reputational consequences when failures reach consumers.

"It is a particularly complex area," says Nicola Smith, partner and regulatory lawyer at Squire Patton Boggs. "There are certain categories of product that have their own legislation and their own regimes. Then there are general product safety regulations, which is a catchall for a product that isn't specifically covered by its own regime."

In Europe, the automotive sector is governed by Regulation (EU) 2018/858, obliging manufacturers to recall any vehicle found non-compliant or unsafe. Broader consumer protections come under the General Product Safety Regulation (EU) 2023/988, which also covers related parts and accessories.

Data indicates the burden is growing: Sedgwick's *Recall Index* reported a 46.3 per cent quarter-on-quarter increase in EU and UK automotive recalls in late 2024.

Yet despite rigorous testing regimes, recalls are still rising.

Imaget: Jonathan Weiss / Shutterstock.com

The Tesla Cybertruck has been recalled eight times since its launch

Volvo, for instance, carries out up to 250 physical crash tests per model, supported by more than 80,000 virtual simulations annually. But as Smith points out: "It all distils down to one question: is this product a safe one in terms of the legally mandated requirements? If it's an obvious risk, it is not a safe product. Therefore there is an obligation to notify and to take corrective action, such as recall."

In 2024, recalls across all sectors in the EU and UK reached a record 14,484, up from 12,503 in the previous year. Food and beverages remain among the most exposed categories, with 5,426 recalls in 2024 – a 12.2 per cent increase year-on-year and the highest in a decade. Regulation here is particularly layered: the EU's General Food Law, its hygiene rules and labelling directives and in the UK the Food Safety Act 1990 and Food Information Regulations 2014. The Food Standards Agency monitors compliance, but accountability still rests squarely with the producer.

The food sector highlights the supply chain challenge. "If your ingredients are supplied by third parties, you will label your food based on the information your suppliers have given you," says Smith. "And you should build in measures like supplier monitoring, supplier audits, quality control checks and testing of products in certain circumstances." Failures in these chains drive complex liability disputes – with insurers, manufacturers and retailers often contesting responsibility for costs.

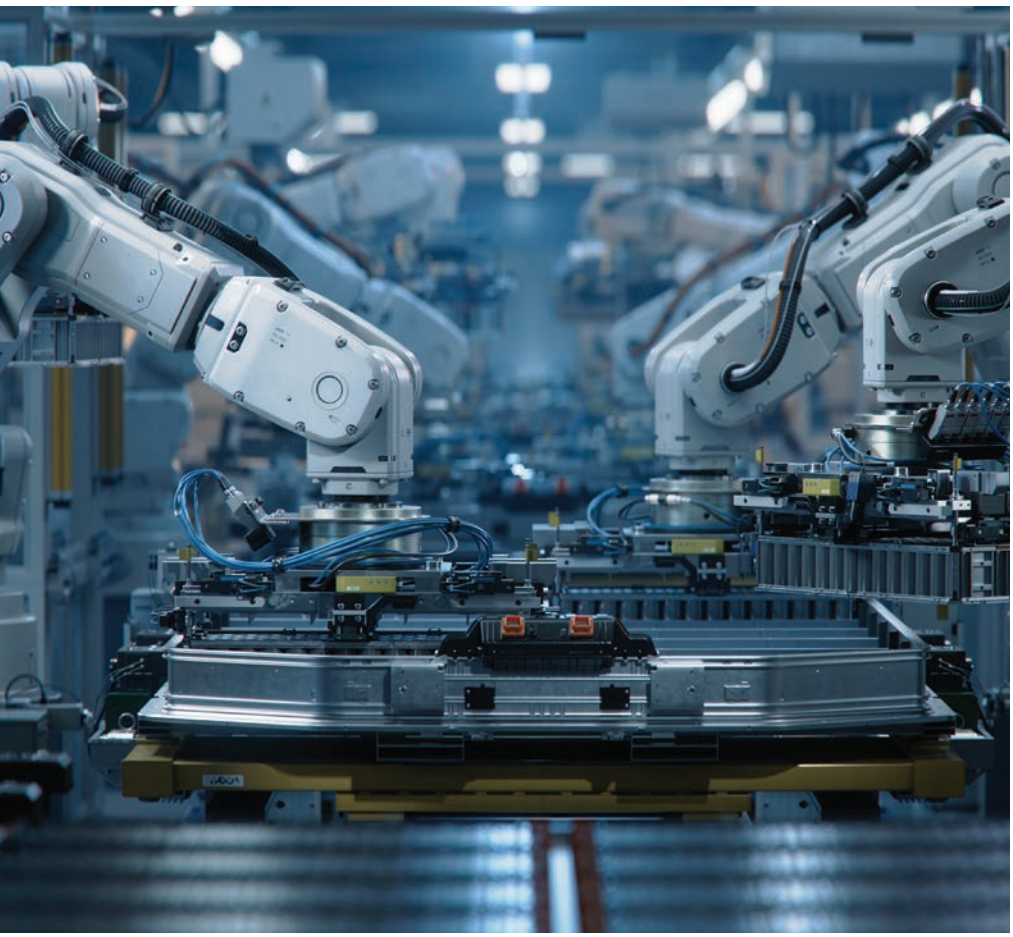
Recalls rarely achieve full recovery. "It's very unusual for all of the products to be returned," Smith notes. And for suppliers, contractual allocation of costs can be brutal. "Typically, the big retailers will have terms and conditions in their agreements stating that if the product needs to be recalled on a reasonable basis due to a defect or a complaint, they have the unilateral right to take that decision and the supplier will pay for it," she explains.

Food and beverages remain highly susceptible to product recalls

The reputational dimension is harder to quantify but arguably more destructive. Volkswagen's 2015 emissions scandal remains one of the most striking examples of product recall fallout. Despite occurring a decade ago, the scandal continues to shape perceptions of corporate trust, regulatory vigilance, and the scale of financial exposure. Total costs – including fines, settlements, buybacks, and vehicle modifications – exceeded the equivalent of over £27 billion, while its reputation index dropped 52 per cent within months, with enduring impacts on sales and brand equity.

This is where reputation management and insurance converge. Product recall insurance is well established, with policies covering direct costs of retrieval, disposal, testing, repair, public relations and legal defence. However, cover is limited: "You can't recover a criminal fine by means of your insurance policy," Smith explains, "but your policy could help you with the costs of legal proceedings around that." Insurers are also increasingly modelling recall risk in terms of supply chain fragility, sectoral loss histories and jurisdictional enforcement differences.

Ultimately, recalls are not anomalies but predictable stress points in interconnected markets. "It's important to look at an issue



The proliferation of electric vehicles has led to a significant rise in automotive sector recalls

globally to determine any risk posed by your product," Smith concludes. "All businesses with worldwide supply chains need to consider the regulations and requirements in each of the countries or jurisdictions where they're supplying their products. And their approaches may need to be different in each of those countries."

Emerging risks are further reshaping the product recall landscape, according to Sedgwick. The adoption of artificial intelligence in product design and manufacturing, while offering efficiencies, has introduced new safety considerations that require updated standards and testing protocols. At the same time, geopolitical pressures – including trade tensions and the impact of US tariffs – have added uncertainty across global supply chains, complicating the speed and effectiveness of recall responses. Sustainability initiatives, which often involve changes to materials or production processes, present additional hazards if not carefully managed.

Looking forward, businesses face an increasingly intricate regulatory environment, with evolving obligations that make brand protection and compliance more demanding than ever. Sedgwick forecasts that recall activity will remain high, driven by ongoing regulatory updates, the introduction of new technologies that require rigorous testing, and growing consumer expectations for transparency and rapid action in the event of safety issues. Preparedness, both operational and strategic, will be critical for companies navigating this shifting landscape.

European product recalls break records

In 2024, European product recalls reached a record-breaking 14,484 events, marking the sixth consecutive year of growth and the highest annual total on record, according to data compiled by Sedgwick. Each quarter in 2024 saw over 3,500 recalls, with Q4 alone setting a new single-quarter record of 3,903 events. This surge is attributed to:

- Increased regulatory scrutiny: Stricter EU regulations have heightened compliance requirements, leading to more proactive recalls.
- Supply chain complexities: Global supply chains have introduced more points of failure, increasing the likelihood of defects.
- Consumer awareness: Rising consumer expectations for safety and transparency have pressured companies to act swiftly.

Sector-specific insights

- Automotive: The automotive sector experienced a significant rise in recalls, driven by the proliferation of electric vehicles and advanced technologies.
- Food and beverage: Recalls in this sector were often due to contamination risks, with a noticeable uptick in allergen-related incidents. It is worthy of note that the food and beverage sector recorded over 5,000 recalls for the first time, a 12.2% year-on-year increase. The leading cause was non-bacterial contamination, primarily aflatoxins and pesticides.
- Pharmaceuticals and medical devices: Quality control issues and regulatory non-compliance were primary drivers of recalls in these industries.
- Consumer products: Electronics, toys and clothing saw increased recalls, often linked to manufacturing defects and safety hazards.

Source: ***European 2025 State of the Nation Recall Index*****, Sedgwick**

CIR

BUSINESS CONTINUITY AWARDS 2026

The pinnacle of achievement in business continuity, security and resilience

SAVE THE DATE
17 JUNE 2026

London Marriott Hotel, Grosvenor Square, London

In association with

CITY OF LONDON

Sponsored by

HORIZONSCAN
RISK - RESILIENCE - READINESS

Supporters

airmic
ALARM embrace risk
Insurance Today

cirmagazine.com/businesscontinuityawards
@CIR_Magazine #BusinessContinuityAwards

Fault lines

With climate and cyber risks continuing to expand in a multitude of ways, the cracks in global systems are widening. Business interruption cover is having to shift to keep pace with these and other pressures, as Martin Allen-Smith reports

In an era defined by interdependence, digitisation and unprecedented volatility, business interruption insurance faces a critical inflection point. For insurance and risk professionals, the imperative is not merely to comprehend these evolving threats but to recalibrate how policies, capacity and exposures are structured in response.

Within the UK and globally, insurers are actively refining BI wordings to address cyber threats, supply chain disruption and climate-driven losses. Simultaneously, limits and capacity considerations are being re-evaluated, particularly for sectors reliant on technology and global supply networks.

As the scale and nature of cyber threats in particular grows, it is little wonder that such recalibration is necessary when the potential impact of interruption is considered.

Image: Jarek Kilian / Shutterstock.com

Limits and capacity are being re-evaluated in sectors reliant on supply networks

AIG's 2024 *Ransomware Threat Insight* report found that when an organisation's back-up data is affected during a ransomware incident, the average critical business interruption loss of hours increases by 65 per cent, and organisations are two times more likely to pay a ransom if their back-ups are affected.

The urgency of addressing systemic cyber risk is now widely recognised as a priority. Stefan Golling, board member responsible for Global Clients and North America at Munich Re, says: "In today's technology-dependent world, organisations can only be successful if they strengthen their digital defences with robust, multi-layered risk management. Cyber insurance is an effective component in this approach." The insurer adds that it is no longer sufficient to view business interruption purely as a consequence of physical damage; digital failure, reputational impact and operational paralysis now demand equal attention.

Within the UK market, policy evolution has seen the introduction of dependent BI extensions that cover losses arising when systems are taken offline, whether due to voluntary shutdowns or regulatory action, in response to cyber incidents.

Axa XL emphasises this shift, noting that such extensions now account for third-party and regulator-induced downtime – incidents that were previously excluded or contested.

Coverage expands

An example of the expanded coverage landscape took place late last year when Marsh and Tokio Marine Kiln launched a BI product tailored specifically for ports. The move was in response to what Ed Parker, head of special risks at Tokio Marine Kiln, calls "a clear gap in the standard cover available to ports and other cargo facilities", which had been exposed by geopolitical turmoil.

Louise Nevill, CEO of UK marine at Marsh Specialty, adds: "Business

interruption events stemming from geopolitics, trade disruption and weather-related incidents are increasing in their frequency and severity around the world, which is resulting in debilitating consequences for businesses involved in international trade. This new facility offers our port and terminal clients a rapidly available layer of cover to protect their operations and facilitate an expeditious resumption of normal operations when these events occur."

Amid high levels of geopolitical and economic uncertainty and a shifting risk environment, the top three risks of cyber, business interruption and natural catastrophe – but also many of the other perils ranked in the top 10 of Allianz's latest *Risk Barometer* – are particularly complex, unpredictable and interdependent.

"What stands out this year is the interconnectivity of the top risks," says Michael Bruch, global head of risk advisory services at Allianz Commercial. "A change in one – or indeed a mitigating action – might have a knock-on effect on another, and another. Climate change, emerging technology, regulation and geopolitical risks are increasingly intertwined, resulting in a complex network of cause and effect."

Bruch says cyber incidents and natural catastrophes are the two BI exposures companies fear most, followed by fire, machinery breakdown and supplier failure. The push for technological advancement and efficiency is affecting the resilience of supply chains he suggests, adding that, today, a failure or disruption in any segment of a supply chain tends to be more severe, leaving minimal time to respond.

"Automation and digitisation have significantly accelerated processes, which can sometimes overwhelm individuals due to the rapid pace and complexity of modern technology," Bruch adds. "While many organisations strive to implement comprehensive strategies for disaster recovery and business continuity, there remains a concern that contingency plans themselves may be overly dependent on technology, highlighting the need for diverse and adaptable solutions."

Image: blvdone / Shutterstock.com

The pandemic compelled insurers to shift towards more tailored coverage

Globally, the repercussions of coups, pandemics and cyber-physical convergence increasingly compel insurers to shift from static, one-size-fits-all BI wordings toward much more tailored, agility-oriented coverage models. Risk managers are adapting accordingly, by demanding rigorous cyber and supply chain due diligence, advocating for scenario-based capacity modelling and preparing for deeper aggregation analysis. The consolidation of risks in digital platforms and supply networks means that traditional single-event thinking is no longer sufficient and that, instead, the focus should be on designing BI portfolios with holistic systems in mind.

UK businesses have increasingly leaned on broader forms of business interruption cover in recent years, particularly during major events like the Suez Canal blockage in 2021, Ukraine-related grain shortages in 2022, and Red Sea shipping disruption between 2023 and 2024. In these scenarios, the losses were not caused by direct physical damage, but by blocked access, logistical breakdowns, or sudden shifts in trade

Organisations demonstrating strong cyber resilience are better positioned to negotiate BI terms

conditions. These are exactly the types of situations modern BI policies are designed to address.

There is also clear momentum behind newer BI solutions. Parametric policies (which pay out based on predefined triggers like a port closure or delay) and cyber BI cover (which responds to digital disruption across logistics platforms) are gaining traction, particularly among firms seeking faster compensation and wider supply chain protection. Insurers have responded by updating underwriting guidance, expanding BI payout triggers, and placing a greater emphasis on supporting businesses that invest in planning and resilience.

Clear Insurance Management says BI cover has evolved beyond traditional triggers linked to physical damage and the emergence of non-damage BI policies marks a shift toward a more flexible and forward-thinking approach.

It adds that, in tandem, insurers are placing greater emphasis on proactive risk management. They now request more detailed supply chain data, such as the locations of critical suppliers and the digital systems upon which businesses rely. At the same time, policies are being reshaped to incentivise resilience, offering stronger terms to companies that invest in advance planning and mitigation, rather than simply reacting after disruption occurs.

Underwriters now find themselves adjusting premium levels and capacity, particularly in sectors exhibiting high systemic aggregation exposure and unclear interdependencies. Clients demonstrating strong cyber resilience, continuity planning and supply chain visibility are better positioned to negotiate competitive BI terms. Some are bargaining for multi-year agreements to smooth volatility; others are contemplating captives or parametric solutions where traditional BI policies cannot sufficiently capture emerging risk vectors.

Other key steps include better risk forecasting with data tools, with insurers using advanced analytics to spot risks earlier. These tools can predict delays, price spikes, or supply issues caused by events such as bad weather or political unrest. UK insurers, for instance, now use scenario modelling to help businesses prepare for events like trade embargoes or transport blockages.

BI policies also increasingly cover problems at supplier sites, not just the business's own premises. UK manufacturers, especially in electronics, are now mapping out their extended supply networks so insurers can offer cover for indirect risks, such as failure at a secondary supplier (which may supply the business's primary supplier).

The increasingly multi-faceted risks that business now face have brought about a similarly diverse shift in approach by insurers. Where BI once rested on property damage and narrow indemnity periods, the evolving frontier now includes non-damage dependencies, cyber contagion and cascading supply disruptions. Successful BI strategy depends on aligning coverage with insights from scenario modelling and resilience testing.

As insurers and clients alike grapple with this shifting reality, the key lies in turning complexity into clarity. Future standards for BI must be dynamic, informed by aggregate stress modelling, and responsive to a world of tightly interconnected systemic risk. For risk professionals, the opportunity lies in reshaping BI not simply as a financial fallback, but as a strategic resilience tool, recognising that insurance must evolve to remain relevant and effective.

CIR | Risk Management AWARDS 2025

The 16th annual Risk Management Awards

The pinnacle of achievement in risk management

BOOK YOUR TABLE

20th November 2025
London Marriott Hotel, Grosvenor Square, London

cirmagazine.com/riskmanagementawards

@CIR_MAGAZINE #RISKMANAGEMENTAWARDS

Headline partners

irm
Developing risk professionals

THE INSTITUTE OF OPERATIONAL RISK
An IRM Group Company

Sponsored by

AON

HORIZONSCAN
RISK - RESILIENCE - READINESS

Supported by

airmic

ALARM
embrace risk


CIR
BUSINESS CONTINUITY
AWA 2025

BUSINESS CONTINUITY AWARDS 2025

The pinnacle of achievement in business continuity, security and resilience

WINNERS' REVIEW

In association with

CITY OF LONDON

Sponsored by

HORIZONSCAN
RISK - RESILIENCE - READINESS

sky

PlanB Consulting

Supporters

airmic

ALARM
embrace risk

Insurance Today

businesscontinuityawards.com
@CIR_Magazine #BusinessContinuityAwards

2025 winners

Business Continuity/Resilience Manager of the Year
Helen Tang, SmartDCC

Newcomer of the Year
Will Wingfield, National Grid

Global Award
Majid Al Futtaim

Best Contribution to Continuity & Resilience
Baltic Resilience

Lifetime Achievement
Tim Armit, QBE

Diversity Award
Linklaters

Excellence in BC in Manufacturing
Honeywell

Recovery in Partnership Award
Royal Mail

Supply Chain, Transportation & Logistics Award
Horizonscan

Excellence in BC in a Tech Company
Fiserv

Resilient Workforce Award
London North Eastern Railway

Strategy through Partnership
Barnett Waddingham & Dementia UK

2025 winners

Testing & Exercising
Virgin Atlantic

Transformation Award
Sky

Disaster Recovery Award – Physical
Colt

Initiative of the Year
Coca-Cola Europacific Partners

Strategy of the Year
Cummins GSCS & Horizonscan

Cloud-based Services
Crises Control

Innovation of the Year
Databarracks

BCM Planning Software of the Year
CLDigital

Team of the Year
Honeywell

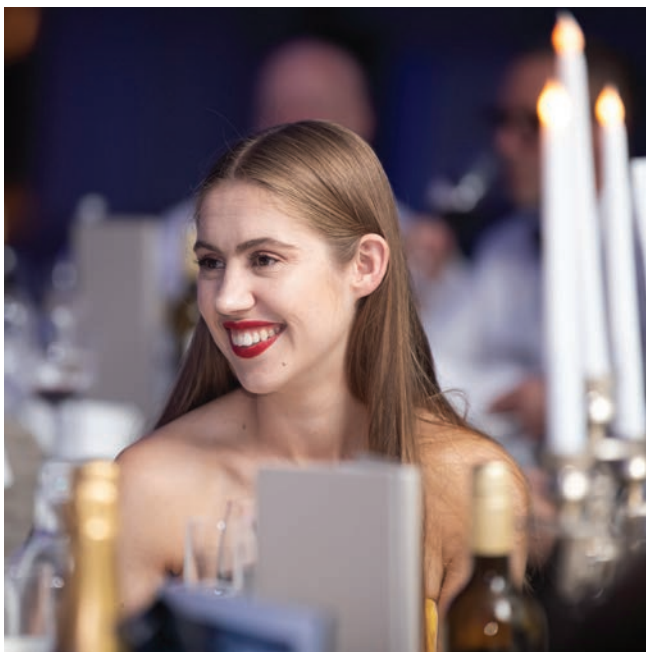
Consultancy of the Year
Insignia Crisis Management

Specialist Company of the Year
Continuity Strategy

Specialist Technology Company of the Year
ISMS.online


WINNER
BUSINESS CONTINUITY
AWARDS 2025
Disaster Recovery Award
– Physical


3



BARNETT WADDINGHAM

Part of HOWDEN

Award-winning resilience, built on partnership

Trusted advice | Long-term thinking | Real-world impact

We're proud to have won the Strategy through Partnership Award at the CIR Magazine Business Continuity Awards 2025. The award recognises the strength of our collaborative approach – supporting organisations to embed practical, sustainable strategies that strengthen continuity and resilience.

This recognition reflects the impact of our work with partners.

SCAN ME
TO READ ABOUT
OUR AWARD WIN

SCAN ME
TO EXPLORE
OUR SERVICES

Strategy through Partnership

WINNER: Barnett Waddingham & Dementia UK

Harshil Shah, partner and head of risk and resilience services at Barnett Waddingham, pictured with Claire Mattinson, head of governance, risk and compliance, Dementia UK; John Benfield, business development manager, Horizonscan; and host Andrew Ryan

The judges said: Recognising that Dementia UK – like many charities – is vulnerable to operational disruptions, Barnett Waddingham designed and implemented a robust BCM framework that embedded resilience into its culture, with strong board-level commitment.

The entry: Barnett Waddingham's partnership with Dementia UK delivered a transformation in business continuity and crisis management. The tailored framework was built around a policy statement, risk assessment and business impact analysis, the creation of ten targeted business continuity plans, and a comprehensive crisis manual. Risks were prioritised through data-driven, collaborative workshops, leading to clear, impact-based planning across critical functions such as clinical services and fundraising. A newly established crisis management team received hands-on training, and a simulated IT outage tested the framework's practicality. Leadership engagement was strengthened through regular governance, policy ownership and strategic integration of resilience into planning. The work drove cultural change, increasing awareness and ownership of continuity planning, encouraging cross-functional collaboration, and establishing annual reviews and simulations. Outcomes included enhanced preparedness, validated response capability, strengthened governance and a future-proofed approach aligned with ISO 22301 standards. This strategic, pragmatic and values-aligned partnership not only protects the charity's operations but sets a benchmark for resilience in the third sector.

Commenting on the win, Harshil Shah, partner and head of risk and resilience services at Barnett Waddingham said: "We are delighted that our partnership with Dementia UK has been recognised with the Strategy through Partnership Award. This accolade celebrates the tremendous commitment shown by both teams in embedding resilience into every level of the charity's operations. It acknowledges the tailored business continuity framework we co-designed, including comprehensive risk assessments, governance structures endorsed at board level and a high-impact IT outage simulation, that has strengthened Dementia UK's ability to safeguard its vital services for families affected by dementia. Winning this award reinforces our belief that a collaborative approach to crisis preparedness delivers sustainable outcomes. It underlines the impact of the training and simulation exercises we delivered, which have equipped the newly formed crisis management team with the confidence and tools to respond decisively to future disruptions.

"Looking ahead, we will continue to support Dementia UK through an annual review cycle, ongoing training and the pursuit of ISO 22301 certification, ensuring it remains at the forefront of best practice. We are proud that our joint efforts have not only enhanced operational readiness but have also fostered a culture of continuous improvement – so that Dementia UK can keep life-changing support flowing to those who need it most."

barnett-waddingham.co.uk/risk-advisory-and-analytics

BARNETT WADDINGHAM
Part of HOWDEN

DementiaUK
Helping families face dementia

WINNER
BUSINESS CONTINUITY AWARDS 2025
BEST CONTRIBUTION TO CONTINUITY & RESILIENCE

SCAN HERE TO FIND OUT MORE

Best Contribution to Continuity & Resilience

WINNER: Baltic Resilience

CEO of Continuity Strategy, Matthew Horrox; pictured with Chris Walker, head of risk management at Durham University; and awards host Andrew Ryan

The judges said: This organisation has built resilience through grassroots collaboration in a region with low continuity maturity, laying strong foundations for lasting impact.

The entry: Launched in 2024 by Continuity Strategy, the Baltic Resilience initiative addresses a critical gap in business continuity awareness across the Baltic states and wider Eastern Europe, where many firms historically lack formal preparedness despite heightened exposure to geopolitical tensions, cyber threats, energy insecurity and social disruption.

Baltic Resilience drives measurable impact through strategic partnerships, targeted workshops, and engagement with local organisations. It was a founding member of the Lithuanian Risk Management Association and works closely with ISM University of Management and Economics to embed resilience education within academic and professional programmes. Practical events, including crisis management exercises and people resilience sessions, have equipped business leaders with actionable skills and led to follow-on initiatives, strengthening organisational and societal resilience. By aligning with EU and NATO regional security initiatives, Baltic Resilience helps ensure that local firms are prepared for extreme disruption scenarios. This combination of support demonstrates a societal-focused approach to resilience, offering a tangible contribution to elevating standards and safeguarding economic stability in the region.

Commenting on the win, Joe McMahon, CEO of Baltic Resilience, said: "We are thrilled that Baltic Resilience has been recognised with the Best Contribution to Continuity and Resilience Award at the official Business Continuity Awards. This accolade is a major milestone for us and a powerful endorsement of the pioneering work we have been doing in the Baltic region.

"The resilience landscape in the Baltics is shaped by a unique set of geopolitical, cyber, and infrastructure threat dynamics. From energy security to supply chain vulnerabilities and hybrid threats, organisations here face challenges that demand innovative, region-specific solutions. Our mission has been to bring world-class continuity and resilience practices into this context, helping businesses and institutions not only withstand disruption but also strengthen their strategic position.

"This award reflects the passion and commitment of our team, backed by our colleagues at Continuity Strategy, who together combine global expertise with a deep understanding of the local environment. It also highlights the vision and trust of our clients, who have embraced new ways of thinking and invested in building resilience as a long-term capability.

"Looking ahead, we are determined to continue expanding our impact, deepening our partnerships across the region, and shaping the resilience agenda in this strategically vital part of Europe."

balticresilience.com

baltic resilience

CIR WINNER BUSINESS CONTINUITY AWARDS 2024 SPECIALIST COMPANY OF THE YEAR

CIR WINNER BUSINESS CONTINUITY AWARDS 2025 SPECIALIST COMPANY OF THE YEAR

SCAN HERE TO FIND OUT MORE

Specialist Company of the Year

WINNER: Continuity Strategy

CEO of Continuity Strategy, Matthew Horrox; pictured with Michael Calamito from RE:ACT Disaster Response; and awards host Andrew Ryan

The judges said: A truly specialist consultancy that works internationally across a variety of sectors, offering broad expertise and tailored solutions to meet diverse client needs.

The entry: Continuity Strategy helps organisations strengthen operational resilience, crisis management and business continuity to help them thrive in an unpredictable environment. Its team comprises experienced specialists drawn from diverse sectors, including government, financial services and manufacturing, many of whom have themselves led global resilience and continuity functions.

The firm offers a broad range of services designed to enhance clients' resilience capabilities. It delivers analytics and business impact analysis to focus resources efficiently, and supports internal audit and second-line teams through independent assurance reviews using benchmarking and its proprietary Capability Maturity Assessment Tool. The team develops crisis management plans and exercises, ensuring preparedness and providing realistic, engaging testing scenarios. It also evaluates programme efficiency, identifies improvement opportunities, and offers interim management to fill capability gaps.

Continuity Strategy works with clients to map critical services, define impact tolerances, and assess vulnerabilities across technology, data, suppliers, premises and teams, guiding targeted investment and strategy development. Training and awareness initiatives further ensure employees at all levels are prepared to respond effectively.

Commenting on the win, Matthew Horrox, CEO of Continuity Strategy, said: "We are absolutely delighted to have been named Specialist Company of the Year at the official Business Continuity Awards. To win this award for two years in a row is a huge honour, and a fantastic recognition of the excellent work we have been doing to support our clients in achieving their resilience goals – practically and cost-effectively.

"We pride ourselves on being a boutique consultancy that consistently punches above its weight. Our success is built on the dedication and expertise of our team, who bring not only deep technical knowledge but also energy, pragmatism and creativity to every engagement. Winning this award is a reflection of the incredible effort they put in every day to help organisations prepare for, respond to, and thrive through disruption.

"We are also enormously grateful to our clients, whose trust and collaboration make our work possible. Many of them are global leaders in their sectors, and it is a privilege to help them build resilience in such complex and fast-changing environments.

"Looking ahead, this recognition inspires us to keep growing and developing our offering. We are excited to continue innovating, exploring new ways to adapt to changing threat dynamics, integrate new technologies into resilience programmes, better reflect corporations' evolving strategies, and expanding the impact we can deliver for our clients in the years to come."

continuitystrategy.com

Continuity Strategy

Resilience isn't static. Neither are we.

Risk and resilience software that's built for what's next.

CLDIGITAL

CIR

WINNER

BUSINESS CONTINUITY AWARDS 2025

BCM PLANNING SOFTWARE OF THE YEAR

SCAN HERE TO FIND OUT MORE

BCM Planning Software of the Year

WINNER: CLDigital

Ian Wilson, senior vice-president of GRC business development, EMEA, CLDigital, pictured with Colm O'Keeffe, global head of business resiliency, Barings, and awards host Andrew Ryan

The judges said: CLDigital's awareness and handling of scalability challenges adds significant value to its notable offering, making it a robust solution adaptable to a wide variety of organisational needs.

The entry: CLDigital's flagship solution, CLDigital 360, combines business continuity, disaster recovery and risk management into one automated, data-driven framework, moving organisations beyond basic compliance towards proactive resilience. Serving sectors including healthcare, finance and government, the platform evolves dynamically, with over 75% of its roadmap shaped by customer feedback and real-world needs. In 2024, CLDigital introduced Monte Carlo simulations to model complex risk scenarios, helping organisations better assess their tolerance for disruption. A new testing and exercising module streamlines recovery plan evaluations using real-time feedback. Reporting has been upgraded through CLDigital Reports, a user-friendly WYSIWYG tool for creating custom, multi-format, dynamic BCM documents with embedded visuals. CLDigital Signal improves crisis communication by linking mass notification systems directly to continuity plans, ensuring rapid, targeted messaging. CLDigital Flow automates data synchronisation across platforms, integrates with threat intelligence, and triggers incident responses instantly, reducing manual resources, and keeping plans accurate in real time. Aligned with global BCM and resilience standards, CLDigital 360 delivers advanced dependency mapping, automated workflows and intelligent incident response. As a result, users report reduced recovery times, stronger compliance results and increased readiness.

"We're proud to be named BCM Planning Software of the Year," said Tejas Katwala, co-founder of CLDigital. "This recognition reflects our mission to evolve business continuity from a static requirement into a living, data-driven discipline that underpins enterprise-wide resilience.

"CLDigital 360 is built for what organisations need next. In a world where risk moves faster than governance and regulations like DORA demand not just documentation but demonstrable resilience, our platform delivers the clarity, adaptability and assurance required by today's enterprises. With a no-code foundation, organisations can modernise how they manage disruption, align continuity with performance, and shift from episodic planning to continuous assurance.

"Over the past year, we introduced AI-powered capabilities to accelerate decision-making across risk, continuity, and crisis operations. This year, we are advancing automation and launching enterprise-wide testing and simulation solutions that make resilience part of everyday operations. Looking ahead, we're expanding graph-based intelligence and real-time interdependency mapping across services, suppliers and systems. This win reflects the bold vision of our customers – those who refuse to treat resilience as a checkbox. The future of resilience is already in motion, and we're building it together."

cldigital.com

CLDIGITAL


CIR
BUSINESS CONTINUITY
AWARDS 2025
HORIZONSCAN
ALARM

Initiative of the Year

WINNER: Coca-Cola Europacific Partners

The business resilience team at Coca-Cola Europacific Partners; pictured with CIR's Megan Davies, and host Andrew Ryan

The judges said: Cross-functional and strategic, this initiative turned a local issue into a worldwide playbook. Despite geographic challenges, the programme has excelled through successful training and engagement.

The entry: Coca-Cola Europacific Partners is the world's largest independent Coca-Cola bottler by revenue, with over four million customers in 31 markets, serving over 600 million consumers. CCEP's business resilience team consists of a dedicated group of specialists across Europe and Australia.

In early 2024, Barcelona and Catalunya experienced severe drought, prompting local authorities to enforce water restrictions that threatened CCEP's production capabilities. While individual departments and sites had business continuity plans, the company identified a lack of a unified organisational response to such crises. To bridge this gap, CCEP's business resilience team developed a cross-functional Water Scarcity Response Handbook. This initiative involved stakeholders from across the health and safety, supply chain, HR, quality, public affairs, procurement and risk teams. The handbook underpins business continuity during water scarcity events, ensuring readiness and communication, and aligning response across departments.

The initiative resulted in improved organisational preparedness, heightened awareness of water risks, and set a strong example for future risk management projects. The handbook's rollout, starting in Iberia and Australia, demonstrated CCEP's integrated approach and commitment to addressing water scarcity, with positive implications both for the company and the wider community.

Commenting on the accolade, Wilco van Eijk, global director, business resilience at Coca-Cola Europacific Partners, said: "This award recognises the development of our Water Scarcity Response Handbook – an initiative that exemplifies the power of cross-functional collaboration in addressing one of CCEP's most critical strategic risks. Water is our most essential ingredient, and ensuring continuity in the face of scarcity is vital to both our operations and the communities we serve. In response to the severe drought in Catalunya in early 2024, our business resilience team led a rapid and coordinated effort involving enterprise risk management, public affairs, communications and sustainability, supply chain and many other functions. Together, we developed a comprehensive and actionable framework to guide our response to water scarcity events – ensuring alignment, preparedness and continuity across the business.

"Spearheaded by Marta Ventosa in Europe and Catt Tyree in our APS region, this initiative has strengthened our resilience, enhanced internal coordination, and is now being rolled out globally. It stands as a model for integrated risk response and resilience planning across CCEP.

"This recognition reflects the dedication of our teams and their ability to turn risk into resilience."

cocacolaep.com

Beat compliance fatigue

As teams grow, so do compliance headaches.

Spreadsheets, scattered evidence, and constant updates slow everyone down. ISMS.online brings it all together, so your people spend less time chasing checkboxes and more time delivering real value.

ISMS.online makes staying compliant easy, efficient, and stress-free.

That's the io way.

isms·online

Specialist Technology Company of the Year

WINNER: ISMS.online

Pictured with their trophy are Sam Peters, chief product officer, ISMS.online, and Mike Garrett, customer support executive, ISMS.online.

The judges said: This entry demonstrated a clear understanding of customers' pain points, and a practical response to them – combining technical capability with customer support to make long-term compliance accessible and sustainable.

The entry: In its winning entry, ISMS.online outlined how it is tackling the complexity of information security compliance by combining technology, people and process. Its SaaS platform supports over 100 global frameworks, including ISO 27001, GDPR and SOC 2, and is designed to make compliance more manageable, particularly for mid-sized organisations and those scaling internationally.

ISMS.online reports a 100% success rate in helping customers achieve ISO 27001 certification via its Assured Results Method – an 11-step framework supported by pre-written policies, and the Virtual Coach, which offers practical guidance through videos and checklists. This level of embedded support, combined with a risk management engine, asset tracking tools and real-time dashboards, creates a clear and practical route through compliance processes that are typically fragmented and manual. Its integration capability is another key differentiator. By plugging into tools including JIRA, AWS and Microsoft, the platform fits within existing workflows rather than forcing complex workarounds. Founded in 2005 and rooted in secure information sharing for UK police forces, the business now serves more than 45,000 users worldwide. ISMS.online also has a long-standing commitment to its own ISO 27001 certification, and its ability to adapt the platform to emerging standards like ISO 42001 for AI governance.

Commenting on receipt of the award, Chris Newton-Smith, ISMS.online CEO, said: "The ISMS.online team is dedicated to helping our customers achieve their compliance goals using an holistic approach that focuses on people, process and platform. Winning the Specialist Technology Company of the Year award at the official Business Continuity Awards is testament to the team's incredible commitment and the support of our loyal customers.

"It's also a reminder of the hard work that goes into achieving compliance with best practice standards and regulations like ISO 27001, GDPR, SOC 2 and more. Businesses across the globe contend with increasing regulatory scrutiny and evolving cyber threats. ISMS.online is proud to support our customers as they rise to this challenge and establish themselves as trustworthy, secure frontrunners in their respective sectors.

"Looking to the future, we're continuing to evolve the cutting-edge ISMS.online platform, with additional AI capabilities, new and improved features and additional standards. We're growing our bank of standard-specific content to support our customers as they streamline their compliance, scale their operations and unlock key competitive advantages that come with demonstrating robust compliance management."

isms.online

isms·online

Industry views

Dr Matthew Connell is director of policy and public relations at the Chartered Insurance Institute

In association with Chartered Insurance Institute Standards. Professionalism. Trust.

Throughout the 2010s, the most widespread complaint from retail consumers was around price walking – the practice of offering renewal rates that were higher than they would have been for new customers with the same risk profile. The issue became front page news and affected the opinions of many SMEs about the insurance they bought, even though there was less evidence of price walking being such a significant issue in this sector.

In 2021, the Financial Conduct Authority attempted to resolve this reputational issue by announcing rules to ensure that people who were renewing their home and motor insurance were treated in the same way as new customers.

Four years later, we are still seeing headlines like the one *Which?,* published in July, that read: 'Taken for a ride?: Sizeable reductions to car insurance renewal quotes after haggling cast doubt on insurers offering fair value'. And yet the FCA's analysis of insurance pricing, published in August, said that its findings provided "encouraging evidence of reduced price differentials across both the home and motor markets".

So what has been happening over the last four years to create such different reports?

If we look at how the market has developed from the consumer's point of view, a picture starts to emerge. Up to 2021, the practice of price walking was widespread. The subsequent rise in consumers' premiums was not because of price walking, but because of huge increases in the costs of claims – prices that have more recently stabilised. To sum up, consumers became used to seeing higher prices because of price walking, and assumed the practice was continuing when prices went up due to claims inflation.

The CII's Trust Index charts consumer perceptions of how insurers are responding to their loyalty – in terms of the gap between their expectations about the importance of the issue and their rating of their insurer's performance. It shows that after the introduction of the FCA's rules, the expectation gap actually worsened – but that as prices have stabilised, it has started to narrow.

This improvement could be the beginning of the solution – but only if insurers demonstrate to consumers what they have shown to the FCA – that price walking is a thing of the past. For example, insurers could offer a reward for loyalty to all their customers – not just those who call in and ask for a loyalty reward. Similarly, insurers are starting to give explicit customer guarantees about pricing: my own home insurer added a message to my renewal quote this summer, writing: "We'll make sure your renewal price is the same or cheaper than you'd get as a new customer for a like-for-like policy."

Insurers have a great opportunity to mend the damage to trust that was caused by price walking. The first step is making pricing policies crystal clear to customers.

Stephen Sidebottom is chairman of the Institute of Risk Management

In association with irm

Risk management has always been about preparing for uncertainty, but the scale and shape of that uncertainty is shifting. Emerging risks that are new, fast-evolving, or poorly understood present distinct challenges; they rarely fit neatly into existing risk frameworks, and often manifest across multiple domains, such as technology, geopolitics, climate and culture – all at once. For organisations, the ability to anticipate and adapt to these risks is becoming more than a defensive necessity and is increasingly a source of competitive advantage.

Unlike well-understood, core risks such as credit defaults or supply chain interruptions, emerging risks are defined by their ambiguity. They may be latent, with no obvious history of losses, or they may stem from weak signals in the external environment. Think of how generative AI moved from niche research to boardroom priority in less than three years, or how the concept of 'quiet quitting' rapidly reframed workplace risks.

Emerging risks also tend to be systemic. Climate change is not just a physical hazard but a driver of litigation, reputational damage, regulatory shifts and social activism. Cyber threats are not limited to technology but cut through governance, culture and national security. This multidimensionality means we cannot treat emerging risks as marginal. They are, increasingly, at the core of strategic resilience.

Traditional risk management has relied heavily on historical loss information, probability distributions and

What's your view? Email the editor at deborah.ritchie@cirmagazine.com

codified controls. These remain essential but are now also insufficient. New skill sets are required to manage uncertainty that can't be modelled with yesterday's data.

Risk managers must be able to detect weak signals and interpret macro trends. This requires familiarity with futures methodologies, scenario planning and structured horizon scanning. The skill is not about predicting the future but about constructing narratives and alternatives that stretch thinking about future possibilities and help decision-makers stress-test strategies. Emerging risks rarely stay in their lane. Skills in mapping interconnections and feedback loops – whether between supply chains, regulatory environments or stakeholder expectations – are essential. A systems thinker can anticipate how a cyber attack cascades into reputational risk, or how a climate regulation alters investor sentiment. The risk professional of tomorrow must, therefore, be comfortable working across disciplines. That means engaging with data scientists, behavioural psychologists, ESG experts and geopolitical analysts. Fluency across these domains helps ensure risks are neither oversimplified nor siloed.

Many emerging risks crystallise through human behaviour: misinformation, insider threats, cultural toxicity or loss of trust. Skills in people risk, culture assessment and behavioural science are becoming vital to detect blind spots that traditional controls overlook. Successful risk management also requires the ability to explain uncertainty to non-specialists, to frame emerging risks in business-relevant language, and to persuade leadership to act. This is perhaps the most important skill of all, as data without narrative will not move a board to invest in resilience.

The priority is to embed these skills not just in the risk function but across the enterprise by investing in training, building teams with a wide range of expertise and perspectives, strengthening governance so that risk managers have independence and access to strategic discussions, and encouraging curiosity in everyone. The most forward-looking companies know that managing emerging risks is not only about avoiding downside; it is about enabling innovation, trust and long-term growth. Those that understood digital disruption early were able to shape new markets rather than defend old ones; those that engage now with AI ethics, biodiversity or demographic change are likely to find themselves not only compliant but leading in reputation and recruitment.

In this sense, the skill most needed is not a technical one, but a mindset: the willingness to see risk management not as a brake on ambition but as a partner in building the future. As the risk landscape evolves, the organisations that thrive will be those whose people are equipped to connect the dots, challenge assumptions, and act before the next wave of change arrives.

Sean Ravenel is a partner at Foran Glennon Palandech Ponzi & Rudloff, a member of Global Insurance Law Connect

In association with GLOBAL INSURANCE LAW CONNECT

Third-party litigation funding has transformed the US legal and insurance landscape since its emergence in the 2000s. Initially facing scepticism due to prohibitions against third-party funding of lawsuits for profit, after the 2008 financial crisis investors seeking returns uncorrelated with volatile stock markets fuelled rapid growth. Some estimates project litigation funding investments at US$18.9bn by the end of 2025, with the global market expected to reach US$67bn annually by 2037.

Litigation funders often back portfolios of mass tort and product liability cases, prolonging disputes and driving over-sized jury awards. Some believe litigation funding encourages weaker claims, drives social inflation and slows settlements. At the same time, carriers are either leaving high risk markets or raising premiums. In commercial auto, product liability and mass torts, claim costs are rising faster than premium growth, as funders enable prolonged litigation or larger settlements.

No comprehensive federal oversight governs litigation funding in the US, but momentum is building. The proposed Litigation Transparency Act would require disclosure of all funding agreements in federal cases. Similarly, the proposed Tackling Predatory Litigation Funding Act aims to "impose a new tax on profits earned by third-party entities that finance civil litigation and curb predatory practices". In 2025, the US Senate Finance Committee considered punitive excise taxes on proceeds from cases using litigation funding, and some states are exploring rules to enhance transparency.

Looking ahead, federal and state initiatives will likely mandate more disclosure to ensure public trust. As capital inflows grow, funders will target complex, high-value disputes, pressuring insurance rates and coverage terms. And insurers will leverage advanced risk modelling, refine exclusions, and explore new coverages, such as adverse judgment insurance for the funders themselves.

Litigation funding is a double-edged sword. Insurers and policymakers must promote fair disclosure rules, invest in robust data analytics, and create a framework that preserves funding's benefits while mitigating its excesses, ensuring sustainability for all stakeholders.

Cautious optimism for AI in claims handling

Insurers are exploring AI to enhance claims efficiency and combat fraud, while making sure that humans remain central, according to a new report from DAC Beachcroft, which is optimistic about the use of AI in the field

Insurers are increasingly optimistic about the potential for AI in claims, with a clear focus on maintaining human oversight and improving efficiency behind the scenes, according to research conducted by DAC Beachcroft.

Training emerged as a critical factor in successful AI adoption, with several organisations having established 'data academies' to help staff interpret results, anticipate assumptions, guard against bias, and detect hallucinations. Human oversight remains key, with staff expected to review and challenge AI outputs to ensure that conclusions make sense. The research suggests that some insurers are already using predictive AI and machine learning to assess loss and detect fraud, while generative AI is still being piloted. Respondents emphasised that humans must remain central to claims handling; few see a fully automated claims process as either likely or desirable. For now, investment in Gen AI is focused on back-office functions – enhancing efficiency rather than replacing customer-facing roles.

Gen AI's ability to address unstructured data was identified as its most significant benefit. "The moment you can do this, you are able not only to make significant improvements to existing models, but also create new models which were out of reach before," one respondent said. Three applications stand out. First, supporting claims handlers with case summaries and call transcripts, allowing them to focus on complex and human elements of their jobs. Second, processing the millions of documents insurers receive annually, extracting relevant information fast. Third, verifying images submitted in claims, with Gen AI able to detect whether photos are genuine, or have been fabricated.

In numbers, 71% of respondents said they already use traditional AI, and 65% reported actively exploring Gen AI. None indicated that their organisation had no plans to adopt AI. Cost savings were cited by 80%, but the most widely reported benefit – noted by all respondents – was freeing colleagues to concentrate on more meaningful work. Legacy systems and imperfect data were highlighted as the main risk by 70%, underscoring the earlier identified need for training and human supervision.

Hybrid approach: Few see a fully automated claims process as either likely or desirable

DAC Beachcroft's research drew on perspectives from a diverse group of organisations, including Axa, NHS Resolution, Zego and the Motor Insurers' Bureau. All highlighted the importance of keeping humans in the loop. Respondents stressed the need for transparency, auditability and clear accountability to ensure responsible AI adoption. The arrival of agentic AI, capable of more autonomous decision-making, is expected to further accelerate change, potentially transforming claims handling within five years.

DAC Beachcroft's report may be read in full at: https://csg.dacbeachcroft.com/ai-in-claims/ai-in-claims-title

Fusion Risk Management
3rd Floor
108 Cannon Street
London EC4N 6EU
United Kingdom

Tel: +44 (0) 20-3884-3538
marketing@fusionrm.com
fusionrm.com
Linkedin: linkedin.com/company/fusion-risk-management/
Twitter: twitter.com/FusionRiskMgmt

Fusion Risk Management is the leading provider of enterprise resilience software that empowers our customers to be agile in times of cascading crises. We help organizations drive the proactive business continuity and risk strategies they need to face growing threats and ensure their operations can bend but not break when faced with any challenge. More than 400 global organizations rely on Fusion's solutions to unify risk across their enterprise, make data-driven decisions, and work seamlessly with their critical third parties to sense risks and mitigate disruptions.

The Fusion Framework® System, Fusion's flagship product, is designed to help organisations proactively manage and mitigate risks. Fusion offers solutions for risk management, third-party risk management, crisis and incident management, business continuity management, and IT disaster recovery. The platform empowers organisations to dynamically see how their business is interconnected and how it can bend but not break when faced with challenges – all from a single, integrated dashboard.

The platform provides intuitive, visual, and interactive ways for organisations to analyse every aspect of their business so that they can identify points of friction, single points of failure, key risks, and the exact actions that they need to take next to mitigate impact. It enables organisations to discover how their business really runs; spot risks, issues, and opportunities for efficiency; and prioritise, take action, measure, and learn over time. Learn more at www.fusionrm.com.

Wavenet Limited
One Central Boulevard, Blythe Valley Park, Solihull,
West Midlands B90 8BG

Contact Name: Chelsea Woodward

Tel: 0344 863 3000
Chelsea.Woodward@wavenet.co.uk
www.shadow-planner.com
Linkedin: www.linkedin.com/company/wavenet_2/
Twitter: X.com/WavenetUK

Shadow-Planner from Wavenet is a multi-award-winning business continuity management software tool, with an award-winning, mobile app that delivers critical information to those who need it, when they need it most.

Shadow-Planner was designed to follow Business Continuity Institute best practice with its comprehensive functionality. Its powerful dependency mapping capabilities (including important business services) allow you to understand any gaps in capabilities via a dynamic graphical dependency map, create plans and playbooks, manage your exercising programme by scheduling planning exercises, capture observations and actions and report on exercises, and manage and monitor your business continuity or resilience programme via a graphical dashboard.

Taking the pain out of the entire process, Shadow-Planner helps your people work smarter and faster so that your business delivers against its resilience commitments efficiently and cost effectively. The reason it stands out in the market, is because it has been developed by business continuity practitioners for business continuity practitioners to support the entire business continuity management lifecycle, from impact analysis and developing strategies and plans, to exercising elements of your programme, through to programme reporting and even mass communications.

Shadow-Planner is based around ISO22301 and the BCI's Good Practice Guidelines and covers the following modules:

- Business Impact Analysis (BIA)
- Strategy
- Business Continuity Planning
- Exercising
- Programme Management
- Mobile Application

BUSINESS CONTINUITY, DISASTER RECOVERY & ALWAYS ON INFRASTRUCTURE

wavenet

Wavenet Limited
One Central Boulevard, Blythe Valley Park, Solihull,
West Midlands B90 8BG

Contact Name: Chelsea Woodward

Tel: 0344 863 3000
Chelsea.Woodward@wavenet.co.uk
www.wavenet.co.uk/
Linkedin: www.linkedin.com/company/wavenet_2/
Twitter: X.com/WavenetUK

You can protect what's most important to your business and recover from any disruptive event, with the help of our services and expertise, gained from 30 years' as a business continuity industry-leader. We help you from identifying risks, managing them effectively and planning and provisioning to continue your operations through all manner of disruptions.

Consultancy Services: Including business continuity, operational resilience, IT service continuity and cyber resilience. Our accredited consultants work with you to produce or validate your BIA, CSA, and security health checks. Advising and consulting on all aspects of your important and critical business operations.

Business Continuity Planning and Third-Party Supply Chain Risk Management: Utilising our award-winning BC software Shadow-Planner, alongside our BCI accredited industry-leading experts, we help you map, mitigate and report on all the dependencies within your risk profile so that you've got everything covered.

Data Protection: Whether you require backup, replication, or a combination of both - with or without recovery, and whether you require self-service, co-managed or fully-managed services, we have the infrastructure, portfolio and expertise to deliver it all – via the cloud, remotely or at any physical location. We also help with testing and rehearsals and documenting your data protection and recovery strategies.

IT & Data Recovery: In times of crisis or for standby situations, we provide Industry-leading data recovery and on demand replacement IT infrastructure delivered either physically to site, virtually or from the cloud.

Work Area Recovery: Whether you need alternative workplaces or standby infrastructure, we offer always-ready workplace positions throughout the UK. Our fully resilient facilities are designed to accommodate both simple and complex working environments. If changes to your work-from-home policy or changes to your real estate footprint have impacted your recovery plans, we're here to provide support in times of crisis and peace of mind for your customers and stakeholders.

BUSINESS CONTINUITY, DISASTER RECOVERY & ALWAYS ON INFRASTRUCTURE

Fortress

Fortress Availability Services Limited
City Reach, 5 Greenwich View,
London, E14 9NN

Tel: +44 (0)20 3858 0099
info@fortressas.com
www.fortressas.com
Twitter: @fortressas
LinkedIn: https://www.linkedin.com/company/fortress-availability-services-limited

The FortressAS team are expert in the provision of Operational and Cyber Risk and Resilience services.

Working along the lines of the NIST Framework, we focus on reducing the risk of disastrous events and mitigating the impact of these events when they do happen.

Our services span:

- Advisory (BC and Cybersecurity)
- Managed Services (Endpoint Detection and Response – ED&R, Virtual CISO)
- Solutions (ED&R, Threat Correlated Vuln Management, Identity, Insider Threat)
- Infrastructure Services (DRaaS, BaaS and Workplace Recovery)

We focus on delivering high quality services and those with a high ROI.

BUSINESS CONTINUITY LOGISTICS

CMAC Business Continuity TRANSPORT

CMAC Business Continuity Transport
The Globe Centre, St James Square,
Accrington, Lancashire BB4 0RE

Contact: Ashley Seed

Tel: +44 (0) 1254 355 126
bctenquiries@cmacgroup.co.uk
www.businesscontinuitytransport.com
Twitter: https://twitter.com/CMACgroupUK
Linkedin: https://www.linkedin.com/company/10540515/

CMAC Business Continuity Transport makes moving your people safely, simple. We believe that everyone should be moved safely, whether it is in an emergency or as a planned exercise. We want everyone to feel secure in the knowledge that if they can no longer work at their usual location, they will be safely moved, just by making one phone call to our 24/7/365 call centre. We were established in 2007 and have become the UK's leading dedicated provider of business continuity transport.

RISK MANAGEMENT SOFTWARE SOLUTIONS

F24

F24
Cardinal Point Park Road,
Rickmansworth WD3 1RE

Tel: 01923 437 784
office_uk@f24.com
www.f24.com
Linkedin: www.linkedin.com/company/f24-uk-limited/
Twitter: x.com/F24UKLimited
YouTube: www.youtube.com/@F24AG/

F24 is Europe's leading SaaS provider specialising in emergency management and critical communication solutions. With 25 years of industry experience, F24 has established itself as a trusted partner for organisations, helping them navigate crises with confidence and efficiency.

FACT24 ENS (Emergency Notification Service) and FACT24 CIM (Crisis Incident Management), are designed to streamline communication and incident management during emergencies. These solutions ensure rapid, reliable alerts and comprehensive tools for managing incidents from start to finish. F24's TopEase® is a comprehensive GRC (Governance, Risk, and Compliance) platform that streamlines corporate governance, enhance risk management, and ensure business continuity through intelligent automation and a holistic view of organizational processes.

F24's offer global reach with local support, ensuring that our clients receive the best service and solutions tailored to their needs. Join the many organisations worldwide that trust F24 to safeguard their operations and ensure business continuity.

RISK MANAGEMENT SOFTWARE SOLUTIONS

ORIGAMI RISK

Origami Risk
12th Floor, St. Clare House
30-33 Minories
London
EC3N 1DD

Tel: +44 (0)1617 917740

info@origamirisk.com
www.origamirisk.com
Linkedin: www.linkedin.com/company/origami-risk/

Origami Risk provides innovative solutions that break down silos, automate processes, and provide data-based context for the decisions risk management, insurance, and safety professionals make every day.

Delivered from a single platform that is fast, secure, and scalable, Origami Risk's RMIS, GRC, EHS, P&C Policy Administration, P&C Claims Administration, and Healthcare risk management solutions incorporate easy-to-use analytics and digital-engagement tools — including portals, dashboards, and reports.

The multi-tenant Origami Risk platform is highly configurable, allowing for seamless integrations with third-party systems and the tailoring of solutions that meet client-specific requirements and workflows without the need for costly, time-consuming custom development.

From implementation expertise to ongoing service focused on your success, Origami Risk solutions are supported by an experienced team that works to ensure you get maximum value from your technology investment.

PROTECHT

Protecht
77 New Cavendish Street
The Harley Building
London W1W 6XB
United Kingdom

Tel: +44 (0) 20 3978 1360
info@protechtgroup.com
www.protechtgroup.com

LinkedIn: www.linkedin.com/company/protechtgroup

Twitter: www.twitter.com/protecht_risk
YouTube: www.youtube.com/user/protechtptyltd

Protecht is an integrated software-as-a-service enterprise risk management solution, supported with training and advisory services, for organisations of any size or geography. Currently on release R11.1, Protecht allows users to dynamically manage all their risks – compliance, incidents, KRIs, vendor risk, IT and cyber risk, internal audit, operational resilience, BCP, health and safety – in a single platform.

Protecht delivers interconnected, structured data through dashboards and reports that can be categorised and documented, allowing users to spot trends and identify areas that require actions. Its reporting tools allow effective and professional communication to risk committees, boards and business stakeholders using customisable visual reports.

The platform is designed to be used across the organisation, with the MyTasks personal dashboard keeping every user on top of their responsibilities, and a mobile app to provide access wherever it's required. Registers can be customised and deployed without the need for coding, and the system's user management functions allow organisations to onboard users and precisely control their access.

With features including a dynamic form builder, the capability to automate notifications and email alerts, and customisable risk assessment scales, Protecht has the flexibility to meet an organisation's specific risk profile. It also includes a wide range of preconfigured dashboards, taxonomies, workflows, registers and analytics relevant for organisations for all levels of risk maturity.

Rather than just being a software company, Protecht is a risk company, incorporating training and advisory services delivered by leading experts in risk management. The product itself, the client implementation process, and the training and advisory services provided to customers are all directly informed by Protecht's understanding of how to manage risk.

www.protechtgroup.com

---

riskHive®

riskHive Software Solutions Ltd
Cilwendeg Mansion, Newchapel,
Boncath, Pembrokeshire, SA37 0EW

Contact: Sandu Hellings
Tel: +44 1275 545874
sandu.hellings@riskhive.com
www.riskhive.com

LinkedIn: www.linkedin.com/company/riskhive
X: @riskHive information
YouTube: www.youtube.com/channel/UCGDHhXKtohhLbmIM37gzF7w/videos

riskHive ERM is an Enterprise Risk Management (ERM) software solution designed to assist organisations in identifying, evaluating, and mitigating risks across their business operations. It provides a centralised platform for real-time risk monitoring and management, enabling informed decision-making and proactive risk mitigation.

Key features include risk identification and assessment, risk scoring and prioritisation, risk mitigation planning, and incident management. Users can define risk categories, assign risk owners, and track the progress of risk mitigation actions. Customisable dashboards and reports provide a comprehensive view of an organisation's risk landscape.

riskHive ERM is user-friendly and can be tailored to specific industry requirements. It seamlessly integrates with existing systems, facilitating data exchange and collaboration between different projects, departments, divisions and/or even companies in very large company frameworks.

Implementing riskHive ERM enhances risk management capabilities, improves decision-making processes, and safeguards company assets and reputation from potential threats.

NATIONAL INSURANCE AWARDS 2026

DEADLINE FOR ENTRIES:
22 October 2025

nationalinsuranceawards.co.uk

Supported by

airmic

ALARM embrace risk

Managing General Agents' Association

Sponsored by

HORIZONSCAN
RISK - RESILIENCE - READINESS

Brought to you by

Insurance Today

In partnership with

CIR

@InsTodayNews @CIR_Magazine #NationalInsuranceAwards

25 March 2026

London Marriott Hotel, Grosvenor Square, London


riskonnect
Can your risk management strategies keep up with the new generation of risk?
Riskonnect's 2024 New Generation of Risk Report surveyed more than 200 risk, compliance, and resilience professionals worldwide on today's biggest threats – and what is being done about them.
Scan the code below to find out how you compare.
AI
riskonnect
Riskonnect.com