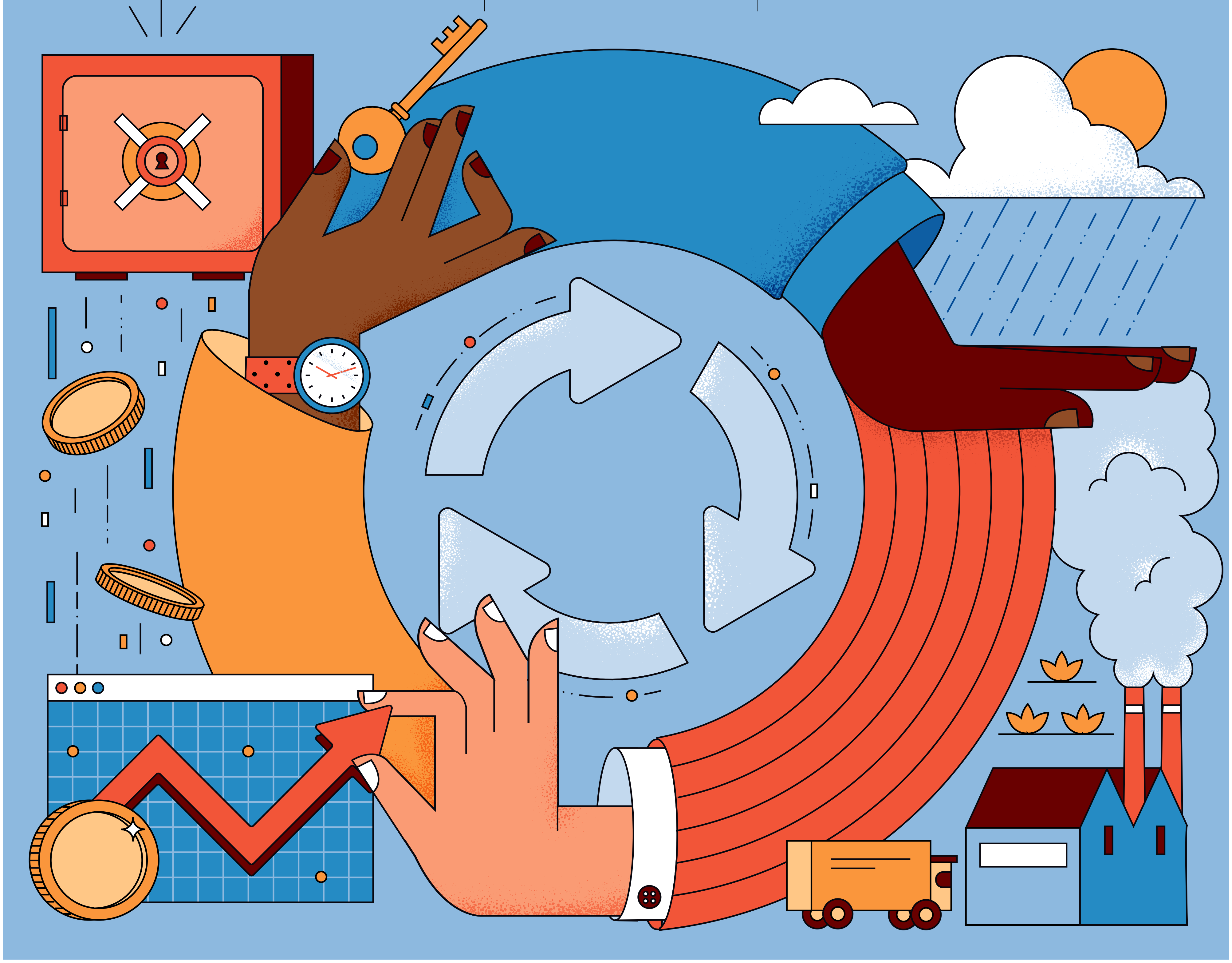
BUSINESS CONTINUITY & RESILIENCE



BUSINESS CONTINUITY & RESILIENCE

Distributed in THE TIMES

Published in association with airmic RESILIENCE FIRST

Contributors

Martin Barrow
A former health editor, news editor, foreign news editor and business news editor at *The Times*, specialising in the NHS and social care.

Simon Brooke
A journalist with 25 years' experience covering business and finance, wealth management and sustainability for a wide variety of outlets.

Ruth Emery
A financial journalist who most recently launched *Times Money Mentor*. Before that, she was deputy money editor for *The Sunday Times*.

Sam Haddad
A journalist specialising in the environment and travel, published in *The Guardian*, *The Times* and the *Economist*'s *1843* magazine.

David Stirling
A freelance journalist who writes news and features for various national publications, including newspapers and business magazines.

Jonathan Weinberg
A freelance journalist, writer and media consultant specialising in technology, business, social impact and the future of work and society.

Raconteur

Campaign manager
Jean-Philippe Le Coq

Reports editor
Ian Deering

Deputy reports editor
James Sutton

Editor
Sarah Vizard

Chief sub-editor
Neil Cole

Sub-editor
Christina Ryder

Commercial content editors
Laura Bithell
Brittany Golob
Joy Persaud

Associate commercial editor
Phoebe Borwell

Head of production
Justyna O'Connell

Design/production assistant
Louis Nassé

Design
Harry Lewis-Irlam
Celina Lucey
Colm McDermott
Sean Wyatt-Livesley

Illustration
Kellie Jerrard
Samuele Motta

Design director
Tim Whitlock

METRICS

Track and analyse to reduce the risk of 'never events'

Effective incident monitoring is key to spotting avoidable accidents and operational failures. Which sectors are getting it right, and how are they doing it?

Martin Barrow

The NHS in England has been collecting and publishing data about so-called never events – serious and largely preventable patient safety incidents which should, by definition, never happen – since 2008. It even boasts of being "one of the only healthcare systems in the world that is this open and transparent about patient safety incident reporting".

It's all done in the hope of learning from any mistakes which do occur – a noble aim, and one that lots of organisations might wish to emulate in pursuit of safer and more effective operations less at risk of incident-related disruption.

Unfortunately, there has also been a steady decline in patient safety standards in surgery in NHS hospitals. On average, at least one patient experiences a potentially life-changing never event during surgery every day across the UK, and many more will also suffer a more minor safety incident that could lead to harm.

In January, a report by healthcare software provider Proximie, in association with leading surgeons, patient advocates, economists and NHS leaders, revealed that the number of never events in the NHS has seen no improvement since 2015, with 407 incidents recorded in the 12 months to March 2022.

Among the report's recommendations was a call for high-quality data to give a clearer picture of what's happening in surgery across the country. Evidence currently available from the NHS is high-level, and much of the data is recorded with pen and paper. Operation notes are usually completed from memory.

Bryn Davies, director of strategy at Proximie, says there is "a golden opportunity to improve patient safety in surgery in the UK".

"If we can make in-depth data available to all surgical teams and healthcare leaders," he explains, "this will allow us to better understand how incidents occur, learn from when things go well and plan strategies to improve patient care."

If clearer data is the key to better incident monitoring, who's getting it right? And how?

Davies thinks there is much that the NHS and other sectors can learn from the aviation industry, for instance, which has a remarkable safety record. "The aviation industry does a huge amount of work to analyse and report on the causes of a crash or a safety incident," he says.

sturti via Getty

"But in NHS surgery, there is no evidence of what has happened in the operating room. That makes it difficult to learn from mistakes."

Dr Sarah Cumbers spent much of her career at the National Institute for Health and Care Excellence, which approves the use of new medicines, treatments and procedures based on data-led evidence. Now director of evidence and insight at the Lloyd's Register Foundation, a global safety charity set up to promote higher technical standards, Cumbers champions the wider use of data by businesses to embed evidence-based approaches to safety.

"It is shocking how far behind some sectors are in this area," Cumbers says. "The pharmaceutical industry has had a strong incentive to produce evidence that its products have an impact on health outcomes. But other sectors don't have the same commercial pressures to demonstrate safety."

That said, things are beginning to change. Cumbers points to HiLo, a maritime risk management specialist which helps shipping companies to share real-time data to improve safety at sea. HiLo has developed predictive analysis tools that warn ship managers of incidents to prevent maritime catastrophes.

"The maritime industry is extremely competitive but HiLo has managed to establish trust in the sector to share anonymised data. This is helping to improve safety," Cumbers explains. Such a strategy is dependent on the latest technology. AI and machine learning can process vast amounts of real-time information across multiple territories, potentially enabling businesses to optimise safety and efficiency much more aggressively – and faster – than has so far been possible. In a warehouse or factory setting, for instance, data which is generated by wearable devices could be used to inform the development of safer ways of working, particularly for risky processes.

But as the NHS has learned from never events, incident data is only as useful as how it is interpreted and applied. Organisational culture needs to evolve such that data-derived learnings can be shared and understood. Only then can the necessary adjustments to work practices and processes be made. One of the most common issues is that data is often collected and stored without informing material changes within an organisation.

Thankfully, just such a transformation is possible. In 2021, for example, offshore drilling giant Noble Corporation realised that its traditional approach to workplace safety – manually filling out paper records to generate reports – was time-consuming and inefficient, and left the corporation with nothing but lagging indicators.

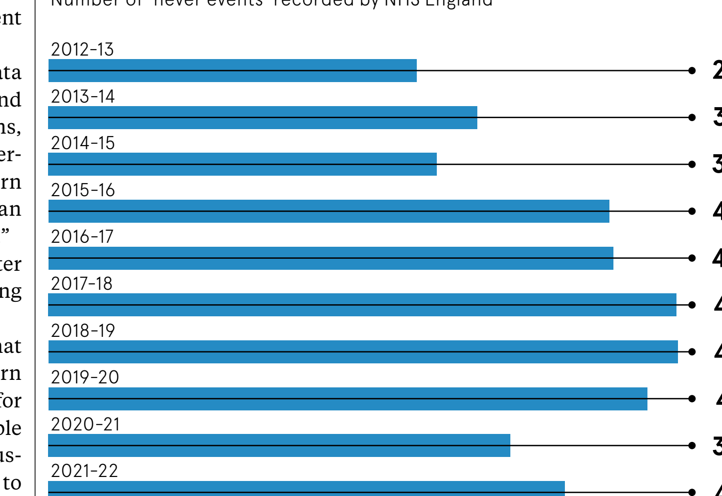
Noble's chosen solution was a piece of software developed by Fennex, a company based in Aberdeen, which uses artificial intelligence, machine learning and cloud computing to monitor critical safety trends and indicators in real time. Quicker decision-making and better health, safety and environmental protection should, in theory, follow, with data submitted from one rig sometimes revealing a bigger pattern of failure when combined with data from others.

And the results have been impressive. Noble has seen a 43% decrease in recorded incidents across its global operations since it introduced the system. Workforce engagement with health and safety initiatives has also increased by 30% and the amount of time to collate incident data has been reduced by 15,000 hours.

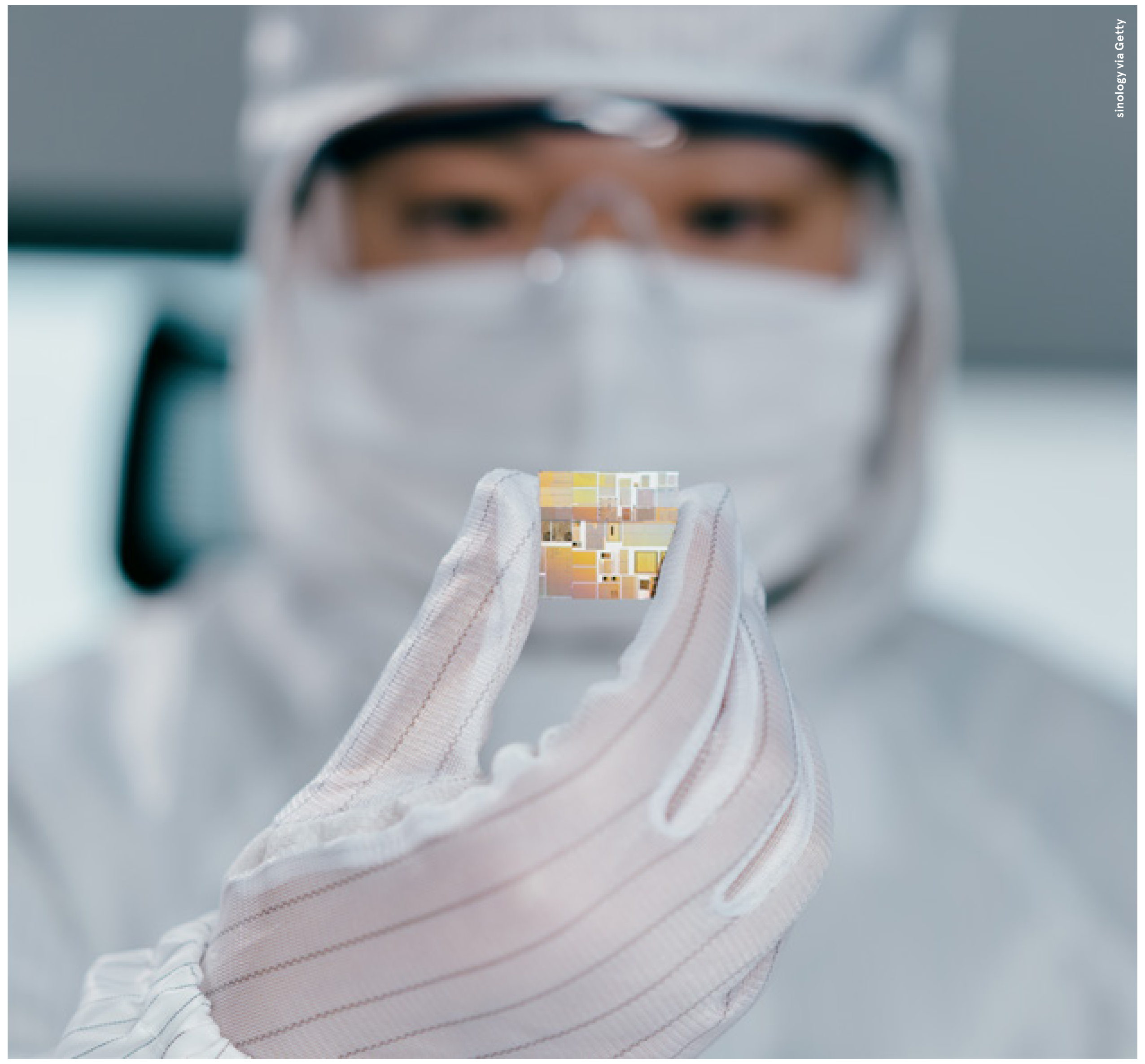
As Fennex director Nassima Brown puts it: "In what is a hazardous industry, quick reporting of risks in more than 30 languages has brought teams together. It has also helped them to work together more safely – and more effectively."

MONITORING OF NHS 'NEVER EVENTS' HAS NOT TRANSLATED INTO A REDUCTION IN THEIR OCCURRENCE

Number of 'never events' recorded by NHS England



NHS England, 2022



sinology via Getty

STANDARDS

Going for gold

It is easier to restore activities after a catastrophe event if best practice is followed. Cue ISO 22301, the independent standard prized by businesses and government departments

Jonathan Weinberg

Among those responsible for business continuity and risk management, the saying "forewarned is forearmed" is apposite. Some choose to go the extra mile to prove their company's level of preparedness by obtaining independent certification of it.

The British Standards Institute's ISO 22301 mark is often hailed as the gold standard of robust business continuity management systems (BCMS) in the event of catastrophes such as natural disasters, terrorist attacks or power blackouts.

Samsung's chip-manufacturing campus in South Korea recently gained the certification – an important step, given the disruptions in the semiconductor industry over the past couple of years. Microsoft is the first hyperscale cloud service to earn the certification, describing it as the "highest available international standard" for enterprises and governmental organisations.

But reaching ISO 22301, introduced in 2012, is not just for the technology giants. It usually takes more than a year for those large organisations to complete the process, but smaller companies can do it in three to six months.

Former Army officer Chris Butler is head of resilience and continuity consulting at Databarracks and has expertise in the UK's high-hazard energy sector, supporting those on the front line in nuclear power plants. Butler thinks that ISO 22301 is appropriate for everyone, from those in regulated sectors such as finance, healthcare and national infrastructure, to those providing critical business services to organisations in complex supply chains.

"You need to show how business continuity fits in with wider business practices such as risk management, information security and disaster recovery," he explains.

"These other disciplines also have their own BC requirements, and it means accreditation is rarely – or shouldn't be – a tick-box exercise. It requires a dedicated, trained team, preferably led internally but supported by external consultants if needed, to implement the necessary actions to become certified."

Butler warns that leaders must be clear about why they need such certification. Is it to prove resilience to customers; to win contracts; or just seem a good idea to have it? "The leadership team needs to embrace the why, the concept and the approach, otherwise the resource will likely be wasted and diluted. There needs to be a board-level champion with the support of execs," he advises.

Graham Brown has worked with government departments to manage crisis events. He is the owner and director of Strategic Continuity, a consultancy that guides clients through ISO 22301 certification and managing their business continuity management systems.

"It's becoming increasingly important for companies to have an ISO 22301-certified BCMS," he says. "It helps them to identify and mitigate key risks. It ensures that controls and processes are implemented to manage the disruption from major incidents. And it enables firms to safely maintain operations, so their customers receive the level of service that they expect."

Such best practice frameworks are especially effective in terms of unexpected threats, Brown suggests, helping to aid a more rapid recovery. "Companies are so invested in ISO 22301, especially post-Covid. They recognise the importance of implementing a robust BCMS that helps to deliver customer and stakeholder confidence. That serves to improve brand reputation, which provides a competitive advantage."

Both Brown and Butler believe the most effective business continuity comes through a focus on ensuring cross-functional business relationships within teams to manage risks.

"Companies need to build a solid community of practice across their organisation in order to create, develop and maintain staff familiar with and competent in the practices of BC," Butler suggests.

"They don't by any means need to be dedicated BC staff, but familiarisation and training will very much help the overall efforts to embed BC. Embedding is a key feature of ISO 22301 certification."

The process of achieving ISO 22301 often starts with an internal alignment check. This will focus on 22301 for the specific requirements of the standard but also, Butler explains, on 22313, which provides further guidance. Taking these together helps to identify any gaps in the business's BC provisions.

But there is as much work to be done after certification as before, Butler warns. He adds that it is crucial not to overlook the danger of a company's attention and priorities from moving on after gaining certification. "Unless you keep your BC management system up to date, you won't pass the next audit," he advises. "It needs a continuous commitment of resources and capabilities – trained people, procedures, facilities, structures and exercises. And, of course, it requires management commitment to keep this on board-level agendas for monitoring, review and improvement."

Such C-suite buy-in is critical, according to Andrew Pattison of IT Governance Europe. Certification can "sometimes be the easy bit", he says, arguing that the real work starts when it comes to maintaining the business continuity plans. "This means the organisation will need to review and, if required, update its plans, and then ensure there is a comprehensive testing schedule in place," he notes.

"This requires commitment across the organisation, but it bears fruit when you need to invoke the plan. It's at that point that you realise all the effort was worth it, as disruption to your critical services is minimised to a level that the organisation and its interested parties are comfortable to accept."

Of course, the level of effort required to get to that stage will vary. At workplace safety experts EcoOnline, the crisis management division is run by Morten Køpke, a former fighter pilot and airline captain. The company he founded, Pilotech, was acquired by EcoOnline in 2021.

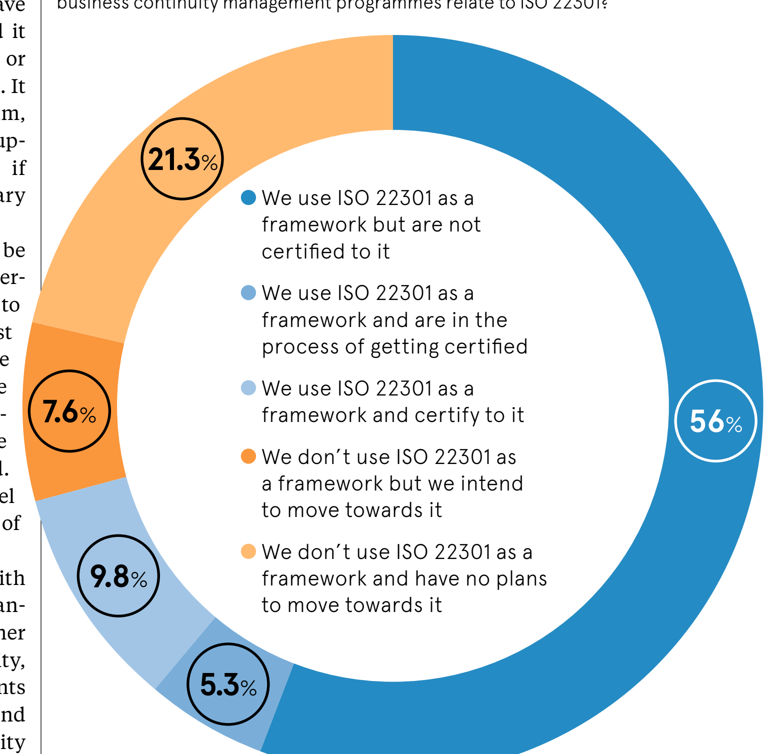
He suggests that for some companies there can be big variations in how difficult it is to have proper business continuity planning procedures and to keep the documents in order. But that isn't a challenge to shy away from.

"Revision of plans, training and exercises make an organisation confident and gives them a culture in which they can handle anything," Køpke says. "This is true BCP and is what ISO 22301 is all about."

> Certification can sometimes be the easy bit. The organisation will need to review and, if required, update its plans

EVEN IF FIRMS AREN'T CERTIFIED TO ISO 22301, IT'S A USEFUL FRAMEWORK

Survey of business continuity and risk professionals worldwide, "How do your business continuity management programmes relate to ISO 22301?"



Business Continuity Institute, 2022

Commercial feature

Are you prepared for the latest operational threats?

Businesses of every stripe need to get to grips with some of the fundamental threats they'll face in 2023, and that means tightening up their operational security

Every second, Twitter publishes 9,500 tweets, adding up to 500 million messages every day. That sounds like a lot until you consider that hosting companies in the capital markets sector are monitoring up to 1.4 trillion data events each day, or 16 million every second.

"For our customers, data loss or downtime isn't an option," explains Stephen Morrow, chief operating officer of Options Technology, which provides secure IT infrastructure to the capital markets sector. "Ensuring consistent access to data and resources means keeping ahead of any potential risk to security or business continuity."

That's no small task in 2023, as businesses in all sectors must be prepared for a range of emerging threats to business continuity. "Over the last 18 months we've seen a series of emerging threats to operational security at the same time customers are facing increasing regulatory requirements to demonstrate that they can manage these risks," says Morrow.

It all means that, to prepare for and mitigate five key risks to operational security in the year ahead, business leaders must review risk assessments and business continuity plans. So, are you ready to handle these risks?

1. Sector-related risk

Last year, there were an unprecedented number of operational security issues in the capital markets sector, says Morrow, but the number and severity of operational incidents is increasing across most industries. "It doesn't matter what business sector you're in, there is some sector-specific risk that you need to manage and be aware of," he says.

Overall, businesses should expect markets to change more quickly and to experience more volatility, says Morrow. This requires companies to speed up reaction times, and to utilise data to increase visibility of market trends and changes. During periods of change, Morrow advises against pausing transformation projects. "What you often see during volatility is that businesses reduce change because they're focused on protecting operations. Everything gets put on hold, which means work gets backed up and projects are delayed. That can have a bigger impact than whatever risk was presented by the volatility in the first place."

Companies should also be boosting communication across the business, adds Morrow. "In many sectors we have been disconnected from our colleagues for two years, and that makes it hard to know your sector inside out, and to see what's changing," he says. "Now's the time to get out there and meet with partners, vendors, clients. Look at how you can be more attuned to the sector, and I think that is best done by talking to other people, face to face."

2. Climate change

Last year, Option Technology's data centres saw record temperatures in some locations, with peaks higher than 40 degrees. "That's a phenomenal temperature, and some servers will shut down between 40 and 50 degrees," says Morrow. "So you're managing that with chillers running at full blast, only to get into winter and have warnings of record cold temperatures."

Many data centres were built at a time when such temperature extremes were not the norm, so plans need to be reassessed and facilities updated. "We replaced two of our chillers this time last year to better regulate the temperature within the data centre. It's also potentially thinking about the servers and what they're able to handle. Are they appropriately distributed within the location?"

It wasn't just data centres that were under strain: last summer Options Technology had to cope with damaged cable which was melting while it was being laid. "We used to worry about the dangers associated with submarine cable and networking, but now it's important to consider where cable is laid because of risks associated with heat and flooding," says Morrow.

Companies must update risk assessment plans in light of changing weather patterns as a priority, says Morrow. Now is the time for businesses to prepare for climate change, if they haven't already. "This is real, it's here, and we need to be prepared for hot summers, cold winters and more frequent flooding," he says.

3. Energy crisis

The second major issue facing organisations is potential instability in energy supply and the rising cost of energy. "In our data centre we have doubled down on our own fuel reserves, so we can run the data centre for as much as six days without external power. We also took on a new generator in direct response to the energy risk, which was a big concern in the last few months," says Morrow.

Be sure you're asking your data centres and IT service providers how they have prepared for potential energy stability. Morrow suggests checking on things like fuel capacity, fuel quality and the frequency of generator testing, to ensure your provider is well prepared.

4. Supply chain risk

With increased supply chain volatility, widespread delays and shortages of components, Morrow says that businesses should consider moving away from just in time supply chains to a 'just in case' model.

The major threat to operational security in 2023 in the supply chain comes from the difficulty many organisations face in sourcing stock. "The chip shortage has had a major impact on our supply chain," says Morrow. "Last year we would be requesting equipment, and someone would call two weeks later and tell you that you could get hold of what you needed, but there would be a 12 or 18 month delay." The result was missing out on potential business because Options Technology simply couldn't guarantee new customers that the right technology could be sourced to support them.

"We completely flipped the model and went and bought a lot of stock," Morrow says. The company standardised on specific products and platforms, allowing them to buy in bulk, and reduce the complexity of procurement. "That has given us a lead over competitors, and for now, our approach is just in case, not just in time."

5. Conflict and geopolitical risk

In some respects, global conflict is the hardest operational risk to mitigate because we are often not in a position to predict or influence global events. What we can do is consider how global instability is affecting not just power supplies but the threat of cyber attacks, and make strong defensive plans, says Morrow.

"In 2023, we are seeing a step change in cybersecurity, with a massive growth in bad actors, state-sponsored actions and cybersecurity attacks and threats," he says. "We need to ensure that every part of the IT infrastructure is hardened, and particularly invest in cyber security training to ensure we're all less vulnerable to attack."

For businesses, this could also mean reconsidering potential cyber-security risks, and taking steps to protect critical data and services with robust back-up policies and patching schedules, Morrow adds.

> Ensuring consistent access to data and resources means keeping ahead of any potential risk to security or business continuity

To find out more visit options-it.com

options

INSIGHT

'Crisis must be managed as a permanent feature'

Resilience is no longer about bouncing back from one disruptive incident. Airmic CEO **Julia Graham** says it's about staying operational in this state of permacrisis

There's nothing new about resilience as a core business topic. In 2014, Airmic published *Roads to Resilience*, which spoke about the need to build greater organisational resilience.

The report also outlined the ingredients for this: a risk radar to provide an early warning system; well-diversified resources and assets to give businesses the flexibility to respond to opportunities as well as adverse or changing circumstances; risk information flows throughout the organisation to prevent 'risk blindness'; response capability to prevent an incident escalating into a crisis; and a commitment to learn from incidents and near misses. The report concluded that organisations should integrate dynamic risk management as part of strategic and operational decision-making.

By 2018, three further principles had emerged: the need to adopt the latest technologies; the importance of identifying and engaging with all stakeholders; and continuously revisiting the organisation's purpose.

Purpose was – and still is – the most important ingredient of resilience. A stated purpose which is out of sync with the organisation's culture, risk appetite and objectives could leave it experiencing a strategic drag when it wants to accelerate, decelerate or change direction. That could become a serious issue in a post-pandemic world where the complexity and connectivity of risks has increased and the pace of change has escalated.

Of course, building resilience is a continuous mission. Even back in 2014, the incentive to become more resilient was recognised as extending far beyond simply avoiding disaster, in that businesses confident in their risk management should have the courage to be more responsive to their customers and the markets they serve. In short, good resilience makes good business sense.

Crisis, on the other hand, has typically been considered as a single bad event, to be met with an event-driven response. But the recent frequency of 'once-in-a-generation events' has shortened the response process and moved the threshold at which something is considered a crisis. In a complex and connected world, a crisis in one part of a business's ecosystem can cause a short-circuit, triggering crises in other areas. A linear response to each crisis no longer works.

We have, in fact, entered a period of instability and insecurity – what you might call a permacrisis. Nowadays, crisis must be managed as a permanent feature, not just a short-term event with a targeted outcome of a return to 'normality'. To put it bluntly, there is no normality any more, and often there is no simple response.

In response to this uncertainty, in December the UK government published its Resilience Framework. Alongside plans to build greater resilience for specific risks, it included plans to strengthen the underpinning systems that provide resilience against all risks. The Framework is built around three fundamental principles: "that we need a shared understanding of the risks we face; that we must focus on prevention and preparation; and that resilience requires a whole-of-society approach".

Addressing a state of permacrisis does indeed demand united engagement and leadership. At a time when global economic optimism is low and governments are suffering from a lack of trust, businesses must constantly re-examine their purpose in recognition of this context. The importance of building trust has never been higher if the disintegration of global networks and supply chains is to be avoided in favour of doing business with smaller and smaller networks of perceived friends, operating closer to home. That idea may ironically offer lower levels of resilience.

The best outcomes can be achieved when governments, regulators and businesses work together in partnership. If businesses can base their actions on honest communications informed by science, with independence from political affiliations, and with consistency, recognising that crisis, like resilience, is a permanent state, to be managed by suitably skilled risk professionals – well, then there is hope. ●

Julia Graham
CEO, Airmic

INTERVIEW

'The more you speak, the more suspicious people become'

For author and academic **Isaac Getz**, it's the companies quietly embracing altruism and social responsibility that are in the strongest position to ride out future disruption

Sam Haddad

A Japanese pharmaceutical company is perhaps not an obvious place to look for a workplace revolution. But in the early 1990s, under the direction of its new president Haruo Naito, pharma giant Eisai quietly began to transform the way it did business. Instead of focusing on the bottom line, from then on Eisai would prioritise what it called human healthcare, first and foremost seeking to relieve the suffering of patients and their families.

Naito invited each department, from sales and marketing to finance, to rethink their business processes with this new goal in mind. For instance, instead of simply trying to sell drugs to doctors and hospitals, the sales teams focused on getting the right products to the right patients, who in the main were suffering from dementia or Alzheimer's.

One sales manager in a poorly performing district, where GPs refused to meet with sales reps, set about educating older people on how to avoid falling – one of the major causes of hospital visits in that age group. She did this through a series of lectures and demos on how to make their homes and habits safer.

A year later, when the manager tried to call the GPs again, they were eager to meet up, having heard good things about Eisai from their patients. The manager doubled her sales in six months. "She didn't do anything to sell, but by changing the way she worked and by generating social value through caring about her clients, the result was economically successful," explains Isaac Getz, professor of leadership and innovation at ESCP Business School in Paris and co-author of *L'Entreprise Altruiste* ['The Altruistic Enterprise'].

This is just one example – from the thousands of businesses Getz has studied over the past 20 years – of a company turning social purpose into stronger business fundamentals, leaving it in a much healthier position in the long term. It is, he suggests, a valuable way to shore up a business against bumps in the road. It's a message that's gaining traction in these uncertain times.

Getz first made a name for himself in 2009, when he coined the term "liberated companies" – that is, businesses which transform themselves to take unconditional care of their employees and become more economically successful and resilient as a result. He outlined these in the book *Freedom, Inc*, which became a global bestseller amid the 2008-09 recession. His ideas were seen as a call to arms, spawning the "corporate liberation movement", whose advocates include the tyre manufacturer Michelin and sports retailer Decathlon.

> It typically takes small and medium-sized companies about three years to transform and large corporations about 10 years. It's a profound thing

Then, in the early 2010s, Getz began to look at the nature of external relationships between businesses, their clients, their supply chain and members of the local community, highlighting networks which thrived when companies did everything they could to maximise the social and environmental value of that ecosystem through mutual trust and authenticity.

In *L'Entreprise Altruiste*, published in 2019, there are examples of companies that have transformed themselves radically for the greater good – and become stronger as a result. Along with Eisai from Japan, there is Handelsbanken, a Swedish retail bank which operates in the UK and provides such good service that its customers often mistake it for a private bank.

During Covid, the bank was working with a UK company making ventilators, which were naturally in high demand, not least within the NHS. When the company placed a large order for parts from overseas, Handelsbanken staff worked evenings and weekends so that it could be processed in seven days, instead of the usual two to three weeks.

"They decided it was a dire situation and therefore important to act for the local community," Getz says. "This bank is very community-orientated, so they did everything they could and then didn't charge extra fees to the client.

"Can you imagine the consequence of that action? How much goodwill it would foster and how people would speak about you to others? It becomes a virtuous circle."

Crucially, Getz explains, it isn't a question of businesses operating in a calculated way – it's about doing what feels right. In a similar vein, Michelin provided free tyres for ambulances in China during Covid, while Sterimed, the French manufacturer of high-end sterile medical packaging, used its logistics expertise to import millions of masks at a crucial point in the pandemic.

Sterimed started by providing the masks to its employees, then gave the 20,000 masks it had going spare to local businesses in the area, and then began to import on a far larger scale for the wider community – a service it provided without making any margin and fronting the production costs themselves. "At that time, mask prices had skyrocketed but Sterimed didn't do it to make money. They did it to serve people," Getz comments.

Of course, that kind of attitude doesn't appear in a business overnight. Getz says it's not so much a change in the way you do business, as a radical transformation and it takes time. "It typically takes small and medium-sized companies about three years to transform and large corporations about 10 years," he says. "It's a profound thing. You can't just go on a training course; you have to transform the nature of the relationships that have been embedded in the organisation since it was founded."

But it is possible to start the journey towards becoming more resilient via clear social purpose. As Getz explains: "It goes back to those processes you've built where your first thought is, 'How can we unconditionally serve this client?'"

> We have a saying in France: 'In fame there is no virtue, and in virtue there is no fame'. There is so much bragging and purpose-washing around

In companies adopting this mantra, he says, the role of the controlling manager disappears, because they become facilitators of social purpose instead. And while you do need a good leader to steer the transition, you also have to involve the majority of your managers and executives for the transformation to work.

For Getz, one of the most positive outcomes from being a genuinely purpose-led business is that it helps with talent recruitment. "We know that millennials see purpose as an important social value," he says. "Ninety percent of job candidates in this group don't want to work for a company that is purely focused on financial and economic profits. They want a social mission and purpose. If you offer that, you will attract a larger pool of candidates than your competitors."

He adds that studies show purpose-led companies also find it easier to retain their top talent, smoothing out the bumps and disruption which high staff turnover can cause. "The research is clear; people are willing to earn less money to do purposeful work, and they're more likely to stay engaged and loyal to a business that does positive things for society instead of being purely focused on making money."

But Getz warns that brands shouldn't shout too much about what they're doing. "We have a saying in France: '*Le bruit ne fait pas de bien, et le bien ne fait pas de bruit*' ['In fame there is no virtue, and in virtue there is no fame'].

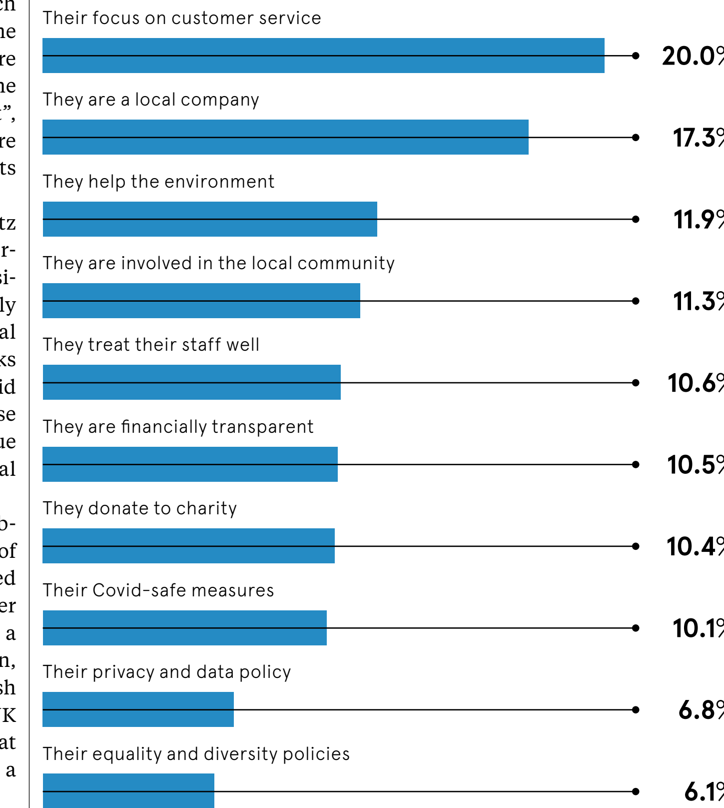
"There is so much bragging and purpose-washing, but the more you speak, the more suspicious people become," he says.

"The companies I've studied didn't tend to speak about what they were doing," Getz explains. "It took me two years – as a researcher, not even as a journalist – to get into Eisai in Japan and meet the president. They didn't want to promote what they were doing, and Handelsbanken were the same.

"Naturally, these stories still come out, employees speak about it on social media and journalists will find out. But they're not doing it for that. They're doing it because they think it's the right thing to do, and they're benefiting in the long run as a result." ●

CHARITABLE AND COMMUNITY WORK ARE HIGH UP CONSUMERS' LIST OF ETHICAL PRIORITIES

Percentage of UK consumers citing the following as key ethical considerations when choosing a business to support



Institute of Customer Service, 2022

ENERGY BILLS AND SMEs

The war in Ukraine put British businesses unexpectedly on the front line last year, via rapidly rising energy bills. That extra cost has proved particularly problematic for SMEs, with 85% having noticed larger bills and three-quarters expecting them to take a chunk out of their profits. In fact, this threat may well be existential; half of SME leaders admit that they will struggle to survive if bills rise any further

51% of SMEs feel they will not be able to continue operating if energy prices keep increasing

11% are already at risk of collapse as a result of the price increases

56% of SMEs are now using less heating and air conditioning because of the rising cost

GetApp UK, November 2022

THREE-QUARTERS OF FIRMS EXPECT PROFITS TO DIP AS A RESULT OF RISING BILLS

Percentage of SMEs reporting the following effects of rising energy prices on company performance

Reduced profits	74%
Increased prices	68%
Reduced investment	39%
Lost competitiveness	32%
Stalled projects	27%
Reduced production	24%
Reduced staff	11%
Other	1%

ABOVE-INFLATION PRICE INCREASES ARE COMMON

Share of SMEs reporting the following percentage increases to energy bills over the past 12 months

Less than 5%	10%
5%-10%	32%
11%-20%	30%
21%-50%	21%
51%-100%	6%
101%-200%	0%
More than 200%	1%

LIGHTS OUT!

Percentage of SMEs reporting power outages over the past 12 months due to supply issues

Yes	52%
No	48%

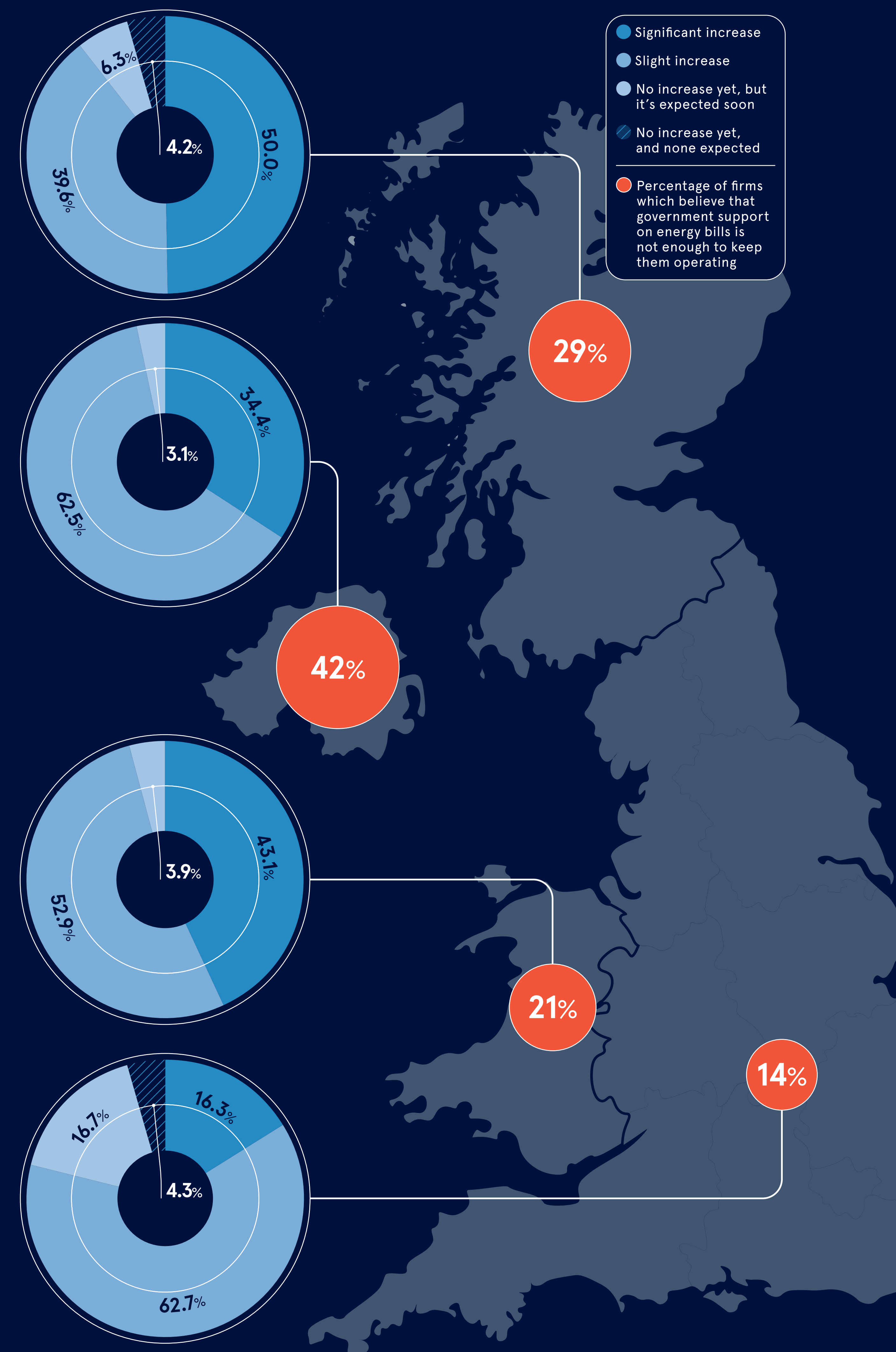
A SIGNIFICANT PROPORTION OF SMEs ARE TAKING MATTERS INTO THEIR OWN HANDS

Percentage of SMEs taking the following measures to reduce the impact of rising energy prices

Installed our own renewable energy system (e.g. solar panels)	31%
Modified processes	51%
Reduced energy consumption	54%
Installed less energy-consuming electrical systems	43%
Stopped production in peak hours	21%

MOST SMEs HAVE EXPERIENCED RISING ENERGY COSTS, BUT SOME ARE FEELING IT WORSE THAN OTHERS

Percentage of SMEs reporting the following degrees of increase to energy bills over the past 12 months



SUCCESSION PLANNING

Protecting what matters

Lasting power of attorney is usually associated with elderly people worried about declining mental capacity. But post-Covid, young entrepreneurs are taking them out to secure their business's future

David Stirling

The unsettling experience of the Covid-19 pandemic led many of us to question long-held certainties, from how and where we worked to the extent to which we could rely on our health.

One of the more pragmatic solutions to these concerns has been an increase in the number of people registering a lasting power of attorney (LPA). These legal documents give a named individual the power to make decisions about someone else's finances if they don't have the mental capacity to do so themselves – because of age, illness or injury.

LPAs usually cover property and financial affairs or someone's health and welfare and can be temporary or permanent. According to the Office of the Public Guardian, which administers the process, 1 million LPAs and EPAs (enduring power of attorney) were established in 2021. This is an increase from the 2020 total, which was 700,000. And towards the end of 2022, the number of LPA applications reached record levels – at more than 4,000 a day.

What's different now, though, is that business owners are increasingly joining this rush to secure LPAs. Sue Wakefield, a director at estate planning firm Zedra, explains that specific business LPAs are a hybrid of the property and financial affairs LPAs and are drafted to cover someone's business interests. Without such an LPA, if a person were to lose the capacity to make decisions then staff and suppliers might not be paid, the bank might freeze business accounts and investors might ask for their money back.

Despite this risk, LPAs have not historically been in high demand from business owners. "Most have tax-efficient wills but they haven't prepared for the possibility of losing their capacity to work," Wakefield adds. "After Covid, business owners recognised that vulnerability. LPA demand has increased, notably among younger entrepreneurs."

Harriet Atkinson is a private client specialist at Bellevue Law. She estimates that pre-Covid, business LPAs accounted for 1% to 2% of LPA enquiries. That figure has now increased to around 20%, she reports. Around 40% to 50% of LPA enquiries from young people are specifically for business LPAs.

"Post-Covid, there's greater awareness among younger people of the potential for incapacity and the impact that could have on business and personal affairs," says Atkinson. "The practical benefit of a business LPA is that it enables a business's continuity, taking care of the company's ability to pay staff, complete transactions and settle tax. But crucially, it will also help to safeguard a business if the owner loses mental capacity." Indeed, a business LPA attorney can also be given the power to wind up or sell the business if the owner's condition is irreversible.

Loss of capacity could be the result of illness or even a physical accident where someone is on strong medication and unable to focus and concentrate. But it may also be because an owner is stranded abroad during a sudden Covid lockdown or geopolitical incident and unable to be present to sign off on a deal or that month's payroll.

Personal grief can also lead to owners struggling to make vital business decisions. Young entrepreneur Samantha Kingston, a co-founder of virtual reality marketing agency Virtual Umbrella, lost her mother in 2018. "I'd never thought about what would happen if something happened to me and my business. But then I experienced mental health issues, depression, burnout – and, of course, grief – while running a business," she says. "In the past year, I've been looking into organising my will. My business partner and I have also spoken about setting up a business lasting power of attorney. I'm 32 and it can feel too soon to be thinking about these things, but it's really important."

Phillipa Bruce-Kerr, a private client partner at Harrison Clark Rickerbys thinks that business LPAs should be used across the board, irrespective of a person's age.

"If you have sufficient assets to think about making a will, then you should be making an LPA," she says. "Sadly, accidents don't just happen to older people. I'm aware of business clients in their late 20s and early 40s who were in car accidents that left them unable to make any decisions. One was for more than 12 months, but the other never recovered their mental capacity.

"You might need help at any time, and you can't predict when that time might be. Covid has made people think they need to do this now."

Bruce-Kerr adds that another factor in this trend is that banks want to see the disaster planning and LPAs that businesses have in place. "If they don't have them, there is a concern that loans are at increased risk," she says. "Post-Covid, there is more focus on whether businesses would be viable during a crisis."

85%

of Brits say they know what an LPA is

16%

mistakenly believe that you lose access to your assets once the LPA is registered

70%

said they do not need an LPA because they are currently healthy

Which?, 2021

Family and friends are usually chosen to act as attorneys for personal matters but for business LPAs the choice is more likely to be a business colleague or peer.

"Not everyone at a senior business level will be comfortable that closer family members have the skills to be involved in running their business," says Bruce-Kerr. "Just relying on your 21-year-old son giving it a go could put your business at risk."

She adds that it is important to understand the nature of the business before taking on this responsibility, particularly where control of the business is not entirely under one person. The attorney named in the LPA only has control over the incapacitated director's shares. The exact details will depend on their contract and the company's memorandum and articles of association.

"The reality of a business owner being unable to continue the day-to-day running of their business is very concerning but often overlooked," says Wakefield. "Who would assume control or have the authority to make decisions if a business owner no longer can?"

If a business LPA is required but none is in place, an application needs to be made to the Court of Protection to appoint a deputy. There is no guarantee that the court would appoint the business owner's preference, and the process is usually time-consuming and costly.

"A business LPA should be an integral part of a business continuity or disaster plan," says Wakefield. "It brings peace of mind to business owners and their families. It has become a necessity."

> "Just relying on your 21-year-old son giving it a go could put your business at risk

From wargaming to gameday: how to harness muscle memory for business agility

Resilience in a crisis is now a vital business skill. And like any skill, it's something which should be trained through targeted exercise

In today's rapidly changing world of permacrisis, stability in business can seem like a distant memory. While many businesses are feeling the pressure of constantly being caught underprepared for disruptive shocks, a new generation of leadership is fueling the strategically adaptive.

These leaders are harnessing the power of business agility. Business agility – a company's ability to constantly assess its operating environment and modify its processes as conditions change – can make organisations more fluid and responsive to unexpected and fast-moving disruption.

For example, an agile business can quickly find alternative sources when faced with a supply chain disruption like the 2021 Suez Canal incident. Similarly, if a vendor's data centre is hit by a ransomware attack, an agile team will quickly put an action plan into motion. With a well-prepared response, an agile business can adapt to fluctuations in the market, new regulations, competitors' price cuts, or the consolidation of its biggest client with a non-customer.

Business agility, then, promotes resilience, which is all about being able to ride out change and disruption and become stronger as a result. It is a never-ending cycle of learning, adapting and responding. However, many organisations still operate as they did a decade ago, making them brittle and unable to flex when the context changes. The traditional top-down approach to crisis, risk and resilience no longer works, as organisations are facing multiple, layered events simultaneously. Failure to embrace business agility could result in poor outcomes, such as employee and customer loss, fines and reduced shareholder value.

The science of business agility

The secret to business agility lies in empowering your people to confidently use their skills and connections to make quick, informed decisions in a constantly shifting landscape. It involves a cultural shift within the organisation and a transformation of how teams, third parties, policymakers and even customers work together.

To achieve business agility, organisations must focus on three key components: context, capability and connectivity.

- Context refers to the ability to gather intelligence about the organisation's threat landscape, markets and society as they evolve. The faster your business can understand the changing operating context, the sooner decisions can be made.
- Capability refers to your people's skill and capacity to assess the change in context, consider the impacts and respond quickly to prevent or minimise disruption.
- Connectivity is crucial in enabling information flow and decisions internally and externally.

The role of risk and resilience

According to a recent study by McKinsey and FERMA, there is room for improvement in predicting events and conducting simulations to assess potential outcomes. Further, only one-third of the respondents indicated that they have effective crisis management measures in place.

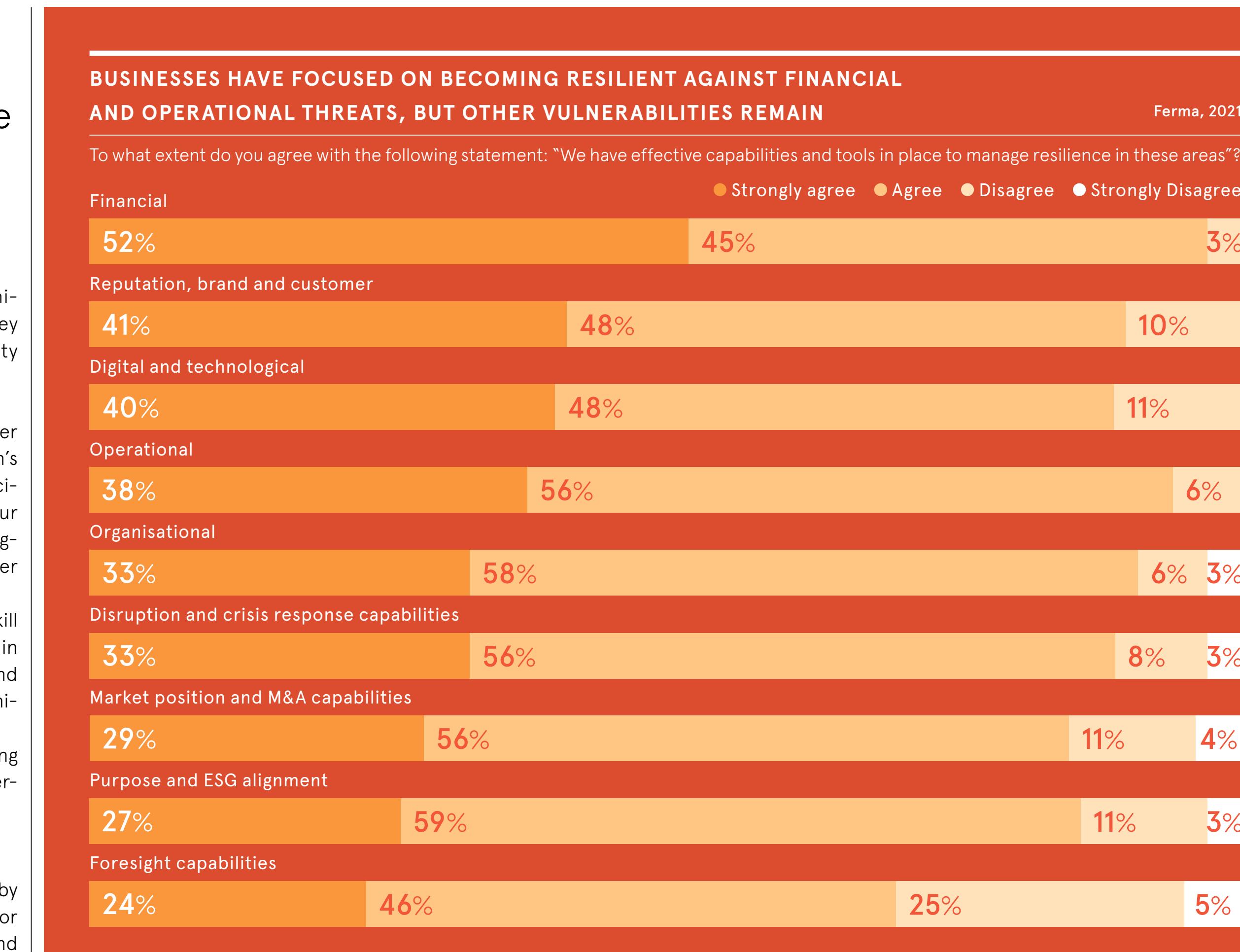
In the new arena of business agility, risk, resilience, and crisis leaders become coaches, building up their team's ability to absorb critical context, analyse it and deploy a coordinated and effective response. Coaches observe, ask questions and see the business from an outsider's vantage point. By spotting hidden and obvious hazards, organisational vulnerabilities and opportunities, resilience coaches develop the people that make up the organisation's agility muscle.

Resilience coaches help the organisation thrive through deliberate practices such as:

- Narrowing the list of scenarios the organisation must plan for and rehearse
- Orchestrating real-life scrimmages to assess the organisation's natural strengths
- Spotting areas for improvement and calculating risks
- Breaking down important gaps and opportunities into fundamentals

These practices are borrowed from industries that deal with binary consequences all the time, such as in sports, the military, aviation, medicine and space exploration. The notion of binary consequences – where there is only one winner and all others lose – is increasingly prevailing in an unstable and highly competitive business world.

Not every team is required to confront terminally dangerous scenarios like running into burning buildings or grappling with lethal space debris, but all teams face rising challenges in their respective fields of work. In such circumstances, these practices can help to build muscle memory for resilience.



Helping organisations bring business agility to life

Iluminr's event rooms combine threat intelligence, strategic risk assessment, simulation insights, response automation and continuous learning capability.

Iluminr simplifies the work of agility-building by giving teams the context, capability and connectivity to carry out engaging and efficient threat intelligence, wargaming and response mobilisation, thereby empowering the entire team to problem-solve simply and effectively.

Through immersive design and gamification, employees gather intelligence, understand its impact on the organisation and make fast, effective decisions, using the same strategies and tools in wargaming as they do a live event.

Iluminr's unique resilience-building approach engages the entire organisation, from the CEO to the shop floor, in short, 15-minute single- and multi-player wargaming scenarios that simulate crises and rapid change, called microsimulations. The library of more than 50 microsimulations includes cyber incidents, third-party disruption, supply chain shocks, extreme weather events, competitive incidents, DEI-related events and more. By participating in these bite-sized games – anytime, anywhere, and even on a smartwatch – teams and third parties gain the skills and the knowledge to respond to real-life business challenges with confidence.

As a situation escalates, teams can use the purpose-built Iluminr app or tap into the power of Iluminr's invisible interface, channeling engagement directly through Microsoft Teams, Slack and other familiar productivity apps to direct real-time insights to decision-makers in event rooms and trigger dynamic response playbooks.

And once the event is over – live or simulated – organisations can also engage their team in post-event surveys and retrospectives to "review the tape", celebrate successes and spot opportunities for improvement.

> "Business agility, then, promotes resilience, which is all about being able to ride out change and disruption and become stronger as a result

Interested in learning more about how Iluminr can help your organisation build its agility muscle starting today? Visit us at iluminr.io/wargamingtogameday

iluminr

OUTSOURCING

A risk worth taking?

A lack of in-house expertise and an eye on the bottom line leads many businesses to hand over responsibility for disaster recovery to external companies. But is it too important to leave to outsiders?

Compassionate Eye Foundation/Robert Daly via Getty

Simon Brooke

According to its fans, business process outsourcing (BPO) is cost-effective and allows companies to access the best talent and the latest technology. The sceptics, on the other hand, would contend that you're bound to end up getting a generic solution foisted upon you and that you'll suddenly discover you're small fry to your provider at the worst possible moment.

That is the fundamental debate about outsourcing, one that is largely unchanged over many years. And yet the market for BPO is reportedly set to grow by 9.4% by 2030, from a baseline of $261.9bn (£215.3bn) in 2022. This is according to Grand View Research, a market research and consulting company. The firm argues that, although Covid-19 threw up challenges, in the longer term more outsourcing is now on the cards but will now include the vital business continuity function.

"BPO companies have changed their business models by restructuring their business continuity plans for a distributed workforce," its experts write. "Businesses have realised the importance of continuous operations planning and disaster recovery to build a more reliable business model that can survive an unprecedented disruption like the Covid-19 pandemic."

With the providers putting in the effort to stay up to date with the way modern businesses are operating, the appeal of outsourcing as an option for business continuity planning is all the more understandable. That's especially true for SMEs, which may not have the resources to prepare their own business continuity planning. It's also relevant for businesses that judge this particular technology and expertise to lie outside their areas of competency. Likewise, businesses in sectors such as healthcare and financial services, which have extensive banks of sensitive data or important intellectual property, may also feel a greater need to call in external specialists to help with organising suitable business continuity procedures.

> Those who choose the outsourcing route need to know exactly what they can expect in the way of support in a worst-case scenario

"It gives you access to the right skills, at the right time," says Asam Malik, a partner and head of technology and digital consulting at Mazars, a consultancy advising businesses on whether to outsource their business continuity work. "You often find someone in the business has been assigned to manage business continuity and they're trying to fit it in late on a Friday afternoon, for instance. They know a little about it, but they might end up becoming a dangerous amateur."

While many SMEs will be inclined to outsource, some may believe they can do it in-house, usually because they have relevant skills and knowledge from their business. DivideBuy, a finance provider which helps consumers spread the cost of their shopping, is one such example. "This is more of an economic approach by a fintech firm in the start-up to scale-up phase," explains the company's CTO, Martin Mitchell. "The pros of in-house business continuity management are that this is bespoke and lightweight enough to keep pace with a rapidly evolving team and business, with low committed costs. The cons are that maintenance and management are more labour-intensive."

Mitchell advises businesses to run their own scenarios to identify vulnerabilities and risk areas and to assess their teams' ability to manage these situations before deciding whether they should outsource. That's because, as he puts it: "Time plus complexity results in failure, whether now or in the future."

Business continuity outsourcing enquiries are certainly increasing at Connectus Group, a business connectivity, cybersecurity and IT support consultancy. Companies want to manage cost, complexity and risk, and do more things more quickly, according to CEO Roy Shelton. "We've seen an upsurge of more than 20% in enquiries between November and January," he adds.

According to research by Connectus Group, the most pressing concern for their clients is the control and security of customer data and internal systems. This has overtaken cost and availability, which were front of mind 12 months ago. "As companies continue to manage hybrid working and the growing threat from cybercrime, it's crucial to make sure that the company's data remains onshore in the UK and that systems remain secure – yet are also accessible to a geographically dispersed team," Shelton explains.

It's important to check your outsourcing partner's IT standards and capability rather than assuming that they use the best on the market. So says David Johnson, service director at payroll and human resource management solutions provider ADP UK & Ireland.

"It's worth considering whether they've made significant investments in IT to enable a high degree of service," he says. "Data and protection are also crucial. Those you're outsourcing to need to be GDPR-compliant and have robust security measures in place. Without this, you're susceptible to loss of data or other scams, which is a huge risk to all businesses."

> There's often a gap between what the client thinks they've outsourced and the service that they're receiving

But Mazar's Malik points out that even if an organisation does outsource its business continuity work, what it can't outsource is risk. Some of this risk could be the result of actions by a third party. A business might know its suppliers and partners and it should have done due diligence on them – but its business continuity provider won't have this familiarity. Even if a company discusses the risks introduced by these third parties, there is no guarantee that the outsourcing party will be willing and able to manage this risk. If they do so, this extra burden will probably be reflected in their fees.

A lack of certainty about the details of the cover and a less-than-clear understanding of the level of service provision is a common problem. "There's often a gap between what the client thinks they've outsourced and the service that they receive," says Malik. "In post-incident reviews we find that clients think that because they have outsourced, the provider is responsible for everything. When things go wrong and the client doesn't think that they've been properly covered, very often the provider will come back and say, 'But you never asked for that – it's an extra.'"

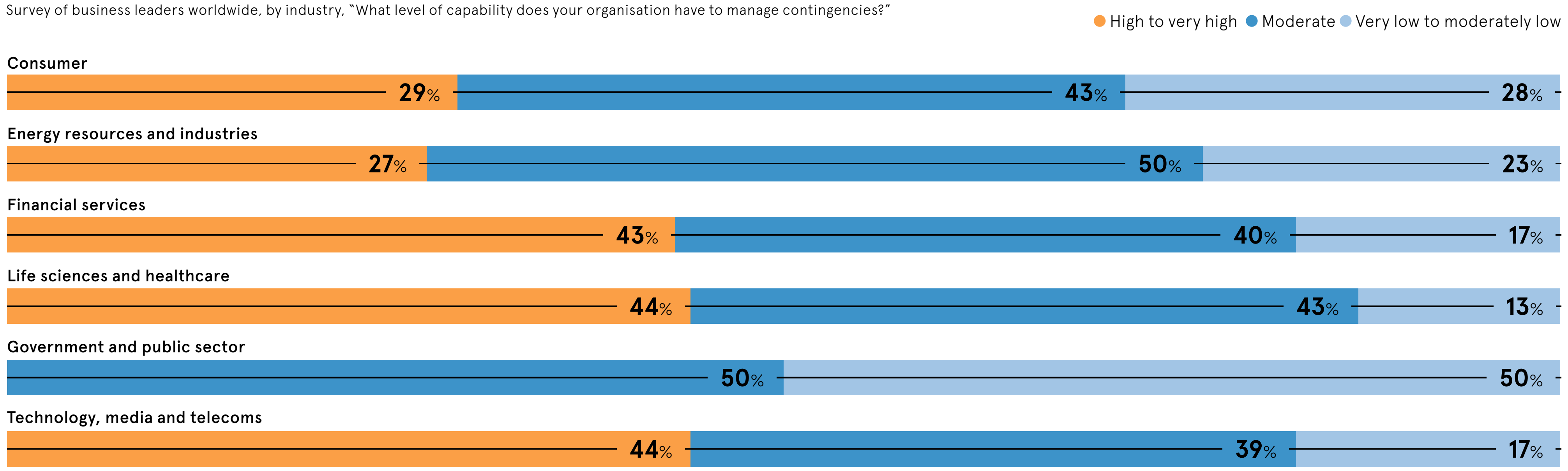
Malik cites a pharmaceutical company that had outsourced to a business continuity provider. A major problem arose and the company was surprised and disappointed when their provider was unable to get the business up and running almost immediately. But the contract had not made any guarantee about timescales. Instead, it made reference to "best endeavours".

Ensuring that your outsourcing partner is big enough to handle your business and can support you in overcoming the interruptions that you might face is important. But this is only one aspect of the capacity question. What if other businesses in your area also suffer disruptions because of a power cut, a cyber attack or a severe weather event? Will sufficient extra office space be available locally? Or will you find yourself in a desperate race to have your provider locate these desks and chairs for you, over and above their other clients based in the same region? Setting up a backup location arrangement through your in-house business continuity systems will avoid such issues.

Ultimately, businesses must weigh the pros and cons of the outsourcing and in-house options for their business continuity, as they would for any aspect of their business. What is apparent, though, is that business leaders who choose the outsourcing route need to ensure that the agreements they make with their provider are clear and that they know exactly what they can expect in the way of support in a worst-case scenario.

SOME INDUSTRIES ARE ALREADY CONFIDENT IN THEIR IN-HOUSE RESILIENCE AND BUSINESS CONTINUITY MANAGEMENT

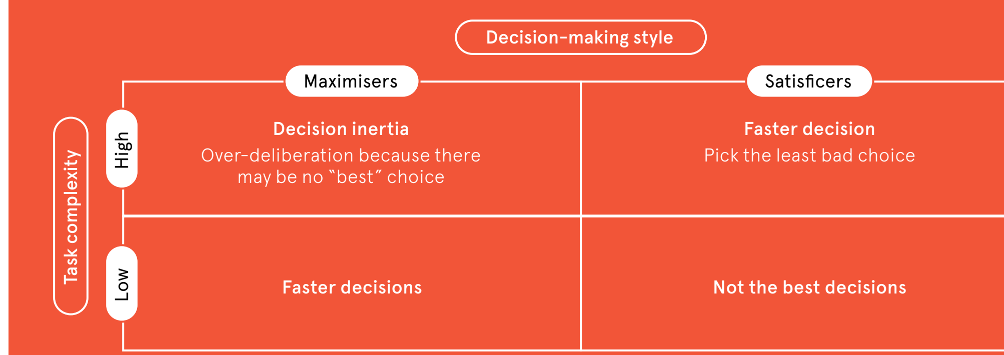
Survey of business leaders worldwide, by industry, "What level of capability does your organisation have to manage contingencies?"



Deloitte, 2022

Commercial feature

HOW DECISION-MAKING DERAILS UNDER PRESSURE



Maximisers are individuals who seek to make the best possible choice and optimise for the best outcome, whereas satisficers are individuals who seek a satisfactory option and are content with making a good enough choice. Realistic crisis rehearsal reveals decision-making style which seminar-style/discussion-based exercises do not.

How crisis exercising fortifies resilience

Conducttr's realistic crisis simulation software allows some of the world's biggest businesses to rehearse their responses to cyber attacks, natural disasters, humanitarian crises and a host of unforeseen events that could derail their operations

It's 3:30pm on a Friday afternoon inside the office of a leading financial company in central London. Staff are sending their last emails of the day and making plans to head to the nearby pub to toast the end of another working week.

Then disaster strikes. The company's entire computer systems are frozen and all employees are locked out of their accounts following a ransomware attack by hacktivists in retaliation for an unethical deal with another company, Building & Co.

The clock is ticking. With each minute that passes, the risk of reputational damage and financial losses increases. Collectively, staff must decide how to protect the reputation of the company while simultaneously making the right decisions to deal with the cyber attack so that their services can continue during the disruption and then return to normal.

Thankfully this is just a rehearsal. It's being run by the financial company itself on crisis simulation software provided by Conducttr. The aim is to give companies realistic rehearsals of potential disasters that could derail their businesses, enabling them to identify and develop decision-makers who can respond quickly under pressure and build formidable crisis response teams.

"Most companies use PowerPoint presentations for their crisis discussions," says Conducttr CEO Robert Pratten. "There is very little interactivity, and staff will do one session per year at most as part of compliance management procedures. When a crisis unfolds, they're unprepared and inexperienced. Panic sets in and they don't know how to respond."

Conducttr sells its crisis exercising software to some of the world's biggest companies and organisations, including the Ministry of Defence and the NHS. Cyber attacks, natural disasters, humanitarian crises and terrorist incidents are among the most common crises its clients rehearse for.

Crucially, the Golden Hour – how businesses respond in the first 60 minutes of a crisis – will often determine whether an event remains manageable or escalates into a full-blown disaster. Fast, effective decision-making is essential and must be developed through regular rehearsals so that decision-making under stress becomes familiar, resulting in a better response.

"Simulation accelerates expertise," says Pratten. "Rehearsing a realistic exercise creates cohesive, experienced teams able to work quickly and efficiently. Many senior leaders worry that they'll look stupid if they get it wrong, but this is because they view exercises as a test. The right mindset is to see exercises as a team-building opportunity where it's safe to fail because the experience and the feedback will help everyone grow as a person and as a team."

The structure and composition of a crisis response team is also critical and shouldn't necessarily mirror the leadership hierarchy of the business. In Conducttr's web series Preparing for crisis, Dave Cope, now senior manager for risk and resilience at Palo Alto Networks, explained: "Having a leadership position within an organisation doesn't necessarily make you a good crisis leader capable of making decisions under pressure."

Businesses must therefore identify employees with the right decision-making skills. There are typically two types of decision-makers: maximisers, who take time to mull over the right choice with the aim of maximising the end goal, and satisficers, who are comfortable making quick decisions that provide a satisfactory outcome, even without the full facts available.

Satisficers are essential during a crisis to avoid decision inertia, when decision-makers freeze and fail to make decisions quickly enough because they fear a negative outcome. In a business crisis, seconds and minutes of inaction can quickly turn into pounds. A survey of IT leaders carried out by IBM found that unplanned downtime can cost $9,000 per minute.

Rehearsing using crisis simulation software will identify satisficers before a crisis occurs. "It's unlikely you'll find out what type of decision-makers you have in your team unless you rehearse the situation," says Pratten. "If you prepare for a crisis in classroom-style discussions, there's no pressure because it isn't realistic, so it won't reveal character."

Businesses can't control when a crisis will occur, but immersive training experiences will give organisations the practice, knowledge and confidence to stop an unforeseen event from spiralling into a disaster that could cost the company its reputation, bottom line and future.

For more information visit conducttr.com/exercising

Conducttr Crisis Exercising Platform

WELLBEING

Invested interest: how money mentoring can help staff – and firms

The cost-of-living crisis is a core business risk, and it's prompting more companies to step up to support the financial wellbeing of staff. But how do you get it right?

Ruth Emery

The link between employees' financial wellbeing and the overall health of a business may not seem obvious.

But how staff feel and think about money – and the state of their finances – is potentially an important (if overlooked) aspect of business resilience. A workforce that is comfortable with personal finances can arguably increase a company's productivity and by extension, improve its bottom line.

According to research by Octopus MoneyCoach, a provider of workplace financial coaching, 95% of employees at the UK's 50 largest companies worry about money, and 80% of employees bring this anxiety to work. The link between money worries and mental wellbeing is well documented. The Money and Mental Health Policy Institute found that two-thirds of employees who are struggling financially show at least one sign of poor mental health. This can include reduced motivation, loss of sleep or poor concentration – any or all of which could affect a person's ability to function well at work.

Meanwhile, a report by the Centre for Economics and Business Research estimates that absenteeism because of financial distress costs UK employers as much as £2.5bn a year.

Julia Turney is a partner at professional services consultancy Barnett Waddingham. She thinks the financial wellbeing of staff plays a huge part in the health and resilience of a business, because "all organisations need people and these people need to be engaged and productive".

She adds: "Poor financial health will result in poorer performance at work. If businesses want to grow, they need to address these concerns and support their employees.

"This is not by any means a new issue. But it has gathered momentum because of the cost-of-living crisis and the economic outlook for the next 12 to 18 months."

It is not only a question of productivity and engagement. Poor personal finances also increase the likelihood of an employee leaving a business to take up a better-paid job.

Low levels of financial confidence may cause staff to make decisions based on headline pay rather than the total value of the employment package. This can lead to a retention headache for companies, creating extra costs and disruption to the business in the long run.

What, though, can employers do to address this issue? In the current climate, they're unlikely to be able to offer significant pay rises and may even be looking to cut benefits to reduce costs. The tight labour market means that employers need to achieve maximum impact from their reward and benefit offerings to retain and attract talent.

The good news here is that there is a growing range of financial wellbeing options to suit all budgets.

Employers should start with an assessment of what kind of help their employees need. Do they need support with day-to-day living costs; how to deal with unexpected events; or planning for future life stages such as getting married, starting a family or retiring?

> My responsibility as CEO is to look after every single person in the firm. Employee wellbeing is a key priority and fundamental in our overall business strategy

The company's pension provider may be a good place to start, as it often provides wellbeing sessions and financial education at no additional cost – and on wider topics than the pension.

HR can play an important part too, by signposting staff to resources around budgeting, debt management and how to deal with a crisis or how to improve financial literacy. The government's MoneyHelper service has lots of free guidance, as do charities such as National Numeracy and StepChange.

It's also worth reminding staff of their current benefits. For instance, if private GP appointments are available, then this might help with any mental health issues that have been exacerbated by financial concerns. A company policy of matching increased pension contributions could help employees feel more confident about their retirement goals.

Considering the age and demographic of employees is a good way to tailor the support the business offers. Mark Pemberthy is benefits consulting leader at HR consultancy Buck and notes that financial education in the workplace has centred on pensions, which is important. "But employers should consider supporting wider financial skills such as budgeting, saving and borrowing," he adds. "This is particularly important in companies with a younger or more financially vulnerable workforce where retirement planning is less of an immediate priority."

Employers can also take steps to help staff get into the savings habit, beyond simply offering a pension. According to research by Buck, 75% of bosses say they would be interested in providing a supplementary savings vehicle on top of a workplace pension, such as a Lifetime ISA or ISA. This compares to 54% of employers in 2018.

Some employers are going a step further too, by offering their staff access to one-to-one financial advice or financial coaching. Research by Octopus MoneyCoach shows that 44% of UK employers would like to offer personalised financial guidance that is tailored to the needs and circumstances of each employee.

The accountancy firm Blick Rothenberg launched a financial coaching programme for its staff, last autumn. This is part of the firm's overall people wellbeing strategy, which has financial, mental and physical strands.

Nimesh Shah, the firm's CEO, explains that this focus on financial wellbeing is partly connected to mental health and the potential implications of that in the workplace. "Financial anxiety has long been a factor of personal stress for a lot of people," he says.

Against the backdrop of high inflation, the accountancy firm has enhanced salaries. But Shah wanted to offer employees something extra. Staff were initially offered one-to-one online financial coaching sessions during work hours, which a spouse or partner could join too. When the benefit was first announced, more than 65% of employees met with a coach.

Employees taking up the scheme then received a year of financial coaching sessions paid for by Blick Rothenberg. For those who wish to continue financial coaching beyond the first year, employees can pay the coaching provider through salary sacrifice, which lowers the net cost.

In addition to the coaching, Blick Rothenberg staff receive free webinars and pension factsheets via their workplace pension provider.

"This initiative is a small part of our commitment to people," Shah says. "My responsibility as CEO is to look after every single person in the firm. Employee wellbeing is a key priority and fundamental in our overall business strategy. It's also useful for talent attraction and retention."

Of course, assisting staff with their personal finances has the potential to come across as patronising. It may also feel intrusive – when did it become a business's responsibility to help employees with their own money issues?

The key here is to ensure the support doesn't feel overbearing or is interfering in employees' personal lives. Creating safe spaces for people to talk about their worries and share meaningful advice and resources can help break down the stigma around financial worries and mental health. It's possible to signpost staff to relevant guidance without becoming personally involved.

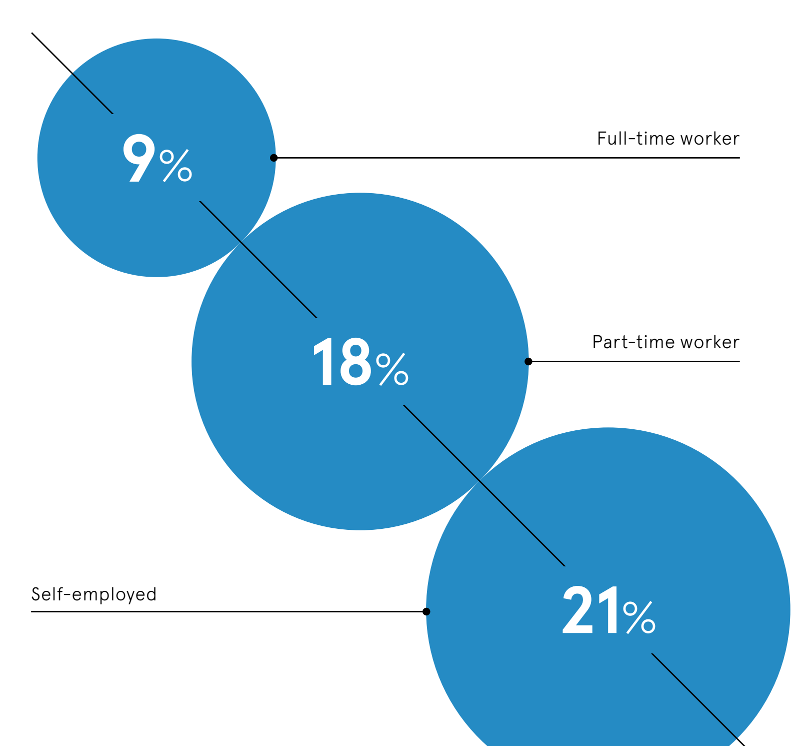
As Anasuya Iyer, vice-president of growth at Octopus MoneyCoach, puts it: "There's so much inertia when it comes to people and money. You need an offering that is easy and exciting to engage with and speaks to employees' individual needs."

The cost-of-living crisis and the fact that today's workforce may have received little or no financial education at school means that many companies now view it as their responsibility to support their staff in this area.

It's a win-win for employee and employer. Supporting employees' financial wellbeing will build their financial confidence and help them to feel valued and more engaged in their roles, ultimately boosting business productivity, resilience and profitability.

EVEN BEFORE THE COST-OF-LIVING CRISIS, THE UK HAD A SIGNIFICANT BASELINE OF IN-WORK POVERTY

Percentage of UK workforce in poverty in 2020-21, by employment type



Department for Work and Pensions, Joseph Rowntree Foundation, 2021

Commercial feature

Why understanding risk and impact must be data-led

Meeting the challenges of the moment requires hard data on what's going on inside an organisation

Times are hard out there right now. With unprecedented challenges over the past few years, inflation running at double digits, recession looming around every corner, and budgets being slashed, the challenge to grow and optimise operations is proving harder than ever for CEOs and their leadership teams.

Market disruptions are happening all the time at an external level – from supply chain disruption to geopolitical black swans – and an internal one, with staff more willing to up and leave for better-paid opportunities elsewhere. It means that understanding your risks and developing and applying effective business continuity strategies are essential to handle these events, whether they're foreseen or unforeseen.

However, far too many organisations build their strategies – and crisis response playbooks to keep them going through the toughest times – on little more than hunches and guesses, rather than hard data and informed insights. They make assumptions of how their business operates based on perceptions, rather than the practical information that passes through their organisation. It's also done at regular, distant intervals, rather than being kept up-to-date as the company adapts.

> With data, we can model disruption and predict the impact to the operations

That's a problem because it can result in false confidence in a business's ability to weather the external and internal storms that come with life in the present day. Business continuity plans were often drawn up for a different era of the organisation, with a different staffing structure. They're riddled with holes because new processes and products have been adopted.

And worse, those issues are only revealed when something goes wrong, and the plans come out of the cupboard and are dusted off – only to be discovered to be barely worth the paper they're written on. The one thing that kills a business continuity plan is change, and the inability to keep up with that.

But there is another way. A data-led approach can continually act as a pulse check for your company, pulling in data to update and inform leaders about the way their business works. "In the world today, data is probably the thing that matters most," says Tejas Katwala, CEO and co-founder of CLDigital, a trusted partner to big businesses in the enterprise risk, government, risk management and compliance (GRC) software space.

"With data, we can model disruption to operations and the supply chain by predicting the impact of a technology failure or a data breach due to a cyber event," says Katwala. "The pandemic taught us that if you only focus on business continuity from a check-in-the-box approach, you have static information that is updated maybe once a year. Insights may well be buried deep in complex documentation that is difficult to parse when decisions need to be made quickly."

CLDigital was set up to look at risk and resilience data in a different way. Rather than seeing it as a check-box exercise, the organisation views data as an opportunity to glean greater insights about how its clients' businesses work. It has developed an operational database that identifies how a company operates by creating data from documents, processes and other elements it is fed, helping clients know better how their company works.

The process is a dynamic, no-code one, meaning it's simpler, lower-cost and less intrusive than traditional alternatives – all of which are likely to be playing on the minds of management at the minute as economic turmoil threatens budgets. "So many risk management solutions today focus on bringing data together from multiple systems, but with CLDigital, the data is connected and adapts to change with no code," says Katwala.

The data model identifies how things happen and change in an organisation, adapting to the way the company operates and helping it adapt to run smoother. It enables companies to incorporate business analytics into their operations whenever they want, wherever they are.

That means companies can build a resilience programme that fits their needs and helps them embrace change. "Boards and executive management need a risk and operations database to proactively manage risks through a strategic lens so they can navigate uncertainty and pivot when the unexpected happens," says Katwala.

To find out more about CLDigital visit cldigital.com

CLDIGITAL


1963 - 2023
airmic
60 YEARS
60 years of leading transformation in risk management and insurance
www.airmic.com
Take a free membership test drive and see what we have to offer.
airmic
Airmic Ltd, Marlow House, 1a Lloyd's Avenue, London EC3N 3AA