Business Continuity Awards
This year's winners have been announced!

Blockchain
Exciting applications for insurance

Artificial intelligence
Legislative change is needed for businesses to benefit

cirmagazine.com

July 2018

CIR
CONTINUITY INSURANCE & RISK

Identity crisis? *Andrew Charlesworth discusses the government's recently published Biometric Strategy*

Closing the gap *The evolving terrorist threat has led to significant shifts in risk managers' insurance needs*

Manufacturing *Ongoing uncertainty surrounding Brexit negotiations has not dulled prospects for the sector*

Lethal weapon

Privacy activism in the post-GDPR world

Industry view: "Cyber governance often fails to reflect technology-driven changes in the way companies are run"

Comment

Intelligent automation could add up to US$512bn to global revenues in the financial services industry by 2020, according to a Capgemini report published this month. It says that with the right combination of robotics process automation (RPA), artificial intelligence (AI), and business process optimisation, the next couple of years could see a lot of change in the sector – with new technologies being implemented not just to drive down costs, but to grow revenue through new customer experiences, and to keep pace with new non-traditional players in an evolving service provision landscape (nearly half suggested that BigTech players, such as Amazon and Alphabet, will be their competitors in the next five years).

The numbers are compelling. The report suggests that already 35% of financial services firms have seen an up to 5% increase in topline growth from automation, with faster time-to-market and improved cross-selling efforts as the key factors influencing gains. RPA deployment alone could help businesses realise a 10% to 25% increase in cost savings, potentially scaling to 30% to 50% with AI-enhanced RPA.

Despite this, adoption of intelligent automation has been slow, with only 10% of companies having implemented the technology at any scale. But for the most visionary and sophisticated, hundreds of billions of dollars in automation-generated revenue is up for grabs over the coming years, if Capgemini's report is on the money.

Others say the real benefits will take much longer to materialise, but not so long that industry can rest on its laurels. "In my opinion, the evolution of automation in financial services will be very similar to the automotive industry revolution in the 70s and 80s," opines head of Swiss Re's Robotic Automation Centre, Jose Ordinas. "The role of humans in processes will dramatically change and [will] focus on things that humans are much better at – in terms of design and problem solving ... leaving the repetitive rules-based stuff to the robots. Though it won't happen in two years, I also know it's not going to take 20 years."

But, as lawyer Mark Deem writes in this issue, for AI to have such a transformational impact, the right regulatory framework needs to be established. He believes one of the key issues is algorithm accountability for when things go wrong; and stresses the importance of ensuring that humans have the ability to override AI decisions and maintain control "because algorithms are created by people and everyone has inherent bias and can make mistakes, unintended and negative consequences could result from artificial intelligence".

There were echoes of these concerns in a speech delivered this month by Financial Conduct Authority chair, Charles Randell.

"Algorithms decide which insurance and savings products you are offered on price comparison websites; whether your job qualifies you for a mortgage; perhaps, whether you are interviewed for your job in the first place," he said. "Some have said that in the future we will live not in a democracy, where the citizens decide how we are governed, nor in a bureaucracy, where officials like me decide, but in an algocracy, where algorithms decide."

Whilst optimistic about the potential of advances in data science, he warns that there is no room for complacency when it comes to governance. As Randell put it: "If we can combine these skills with fair standards and with public trust, we can maximise the opportunities for the UK finance industry to succeed in the global market."

Deborah Ritchie, Editor

FUSION
RISK MANAGEMENT

Realise the Full Potential of Your Programme

Fusion offers solutions to help you solve specific business problems, making your programme more effective, more efficient, and more economical.

FUSION FRAMEWORK® SYSTEM™

With our award-winning software, the Fusion Framework® System™, you'll improve your ability to make data-driven decisions about your business and increase the value of your programme.

Choose Success. Choose Fusion.

fusionrm.com/discover

COVER STORY

Editorial & features

Thinking resilience

News, views & regulars

Closing the gap

The evolving terrorist threat has led to significant shifts in risk managers' needs when it comes to insurance. Ant Gould examines the new dynamics and looks at how the insurance industry has responded to calls for change

Winners' Review 2018

The winners of the 20th annual Business Continuity Awards have been revealed at a Gala Dinner and Ceremony in London's Mayfair. Sponsored by Barclays, The City of London Corporation, ClearView Continuity, CMAC Business Continuity Transport, Daisy, Fortress Availability Services, Fusion, PlanB Consulting, Sungard Availability Services, Yudu and the Retailers' Business Continuity Association, turn to page 29 for the highlights of the industry's main event.

CIR
CONTINUITY INSURANCE & RISK
thinking resilience

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

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

Design & production manager
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

Contributing writers
David Adams
Graham Buck
Ant Gould
Angelique Ruzicka

Accounts
Marilou Tait
Tel: +44 (0)20 7562 2432
Fax: +44 (0)20 7374 2701

Subscriptions
Tel: +44 (0)1635 588 861
perspectivesubs@dynamail.co.uk

£189 pa in the UK
£199 pa in the EU
£209 pa elsewhere

Cheques must be made payable to Perspective Publishing Limited and addressed to the Circulation Dept.

CIR Magazine is published by:

Perspective Publishing
6th Floor
3 London Wall Buildings
London Wall
London, EC2M 5PD
UK

Tel: +44 (0)20 7562 2400

ISSN 1479-862X
cirmagazine.com

At a turning point

Artificial intelligence is poised to have a transformational impact on people, businesses, governments and societies – particularly in healthcare – but we must get the regulatory framework right, says Mark Deem

The development of law has played a pivotal role during fundamental social transition in countries governed by the rule of law – look at civil rights (1950s), anti-discrimination (1990s) and, more recently, privacy.

And now, artificial intelligence (AI) is poised to have a transformational impact on people, businesses, governments and societies – particularly in the healthcare arena, where AI will enable faster diagnosis, and earlier and better intervention, ultimately saving lives.

However, we cannot achieve this transformation under current law. So again, a vital catalyst to the potential of AI will be a suitably robust, yet appropriate, legal and regulatory framework. What's needed is a system that acknowledges how the technology works and affords minimum standards and levels of protection to its participants, whilst being relatively light-touch to encourage innovation and to flex with additional applications of the technology.

One of the key issues is algorithm accountability for when things go wrong, as liability in artificial intelligence is highly complex. It is relatively straightforward to determine the liability where there's a dispute about a bridge, for instance; you look at the design engineers, the product manufacturers and the constructors. In AI the value chain is considerably longer, dispersed and more complicated: from the designer and manufacturer of the core product or software, to the algorithm designer, its coder and integrator. There's also the owner of the data set that has been interpreted as well as the creator of the original data point – and potentially others. As a result, assigning legal responsibility is extremely difficult and will potentially open up the prospect of extensive litigation based on the claims and counterclaims from the range of parties seeking to avoid or minimise liability.

Given the multiple participants involved in any AI value chain, an efficient way of solving the liability problem will be for market players to define the parameters of their own liabilities. This will provide assurance throughout the industry and enable innovation in insurance products to carry liability, which will encourage investment.

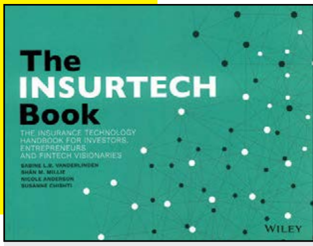
Another vital component of the legal framework will be ensuring that humans have the ability to override artificial intelligence decisions and maintain control over the technology. Because algorithms are created by people and everyone has inherent bias and can make mistakes, unintended and negative consequences could result from artificial intelligence; it could be catastrophic for rogue robots or vexatious vehicles to have legal rights.

"Given the multiple participants involved in any AI value chain, an efficient way of solving the liability problem will be for market players to define the parameters of their own liabilities"

The recommendation of the House of Lords Select Committee on Artificial Intelligence in April to ask the Law Commission to review the adequacy of the existing legal framework was the right thing to do. The end result must be a system that balances the innovative and entrepreneurial aspirations of business with a safety net of protections should systems malfunction. Clearly, it's critical that the review involves input from the technology and insurance industries and it's incumbent upon those sectors to ensure that their voices are heard.

Mark Deem is a partner at law firm Cooley LLP

Inspiration for resilience professionals



The InsurTech Book

Vanderlinden, Millie, Anderson & Chishti. Wiley, 2018. Reviewed by Deborah Ritchie, Editor, CIR

wiley.com

More than 550,000 new start-up businesses were established each month during 2016, of which FinTechs and InsurTechs accounted for 30,000. InsurTech start-ups alone have received US$20bn of investment since 2004. Some 33% of those funded between 2013 and 2015 had a focus on internal insurance processes; 61% by 2016.

InsurTechs are beginning to show how they might re-engineer value chains in insurance, at a time when the industry is looking to keep pace with change – to 'get fit or fail', and this book is a timely guide to all that is exciting in the field.

"The insurance industry talks a good game about InsurTech," says group CEO of AXA, Amanda Blanc, "but the follow up or delivery isn't always there. But it needs to be as this great profession of ours is facing a genuine existential crisis. Our traditional ways of working and servicing our customers are becoming increasingly irrelevant."

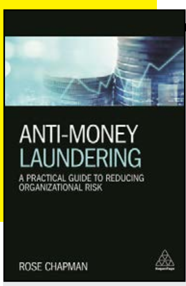
The insurance industry is still very much at the start of the journey, with numerous angles to be explored and opportunities realised.

Following the format of its 2016 title on the FinTech market, the publisher has drafted in expert insight from a huge and diverse pool of contributors, so a lot of ground is covered in this book's 314 pages.

There is, unsurprisingly, a predominant focus on personal lines insurance throughout, but a lot of the theory would still apply to commercial carriers; and some of the core ideas can be (and in some cases are already being) applied in business insurance.

"Following the format of its 2016 title on the FinTech market, the publisher has drafted in expert insight from a huge and diverse pool of contributors, so a lot of ground is covered"

Generic topics including data analytics (data anything, for that matter), claims processes and blockchain, will appeal to most readers – as will, no doubt, some of the new ideas that will inevitably spring forth from this treasure trove of concepts in insurance technology.



Anti-Money Laundering

Rose Chapman, Kogan Page, 2018. Reviewed by Deborah Ritchie, Editor, CIR

koganpage.com

Each year over US$3trn is laundered by criminals on a global scale, threatening the legality of everyday business outcomes. Money laundering is a risk to any organisation engaging in international trade, and it has become a growth industry in recent years – thanks in part to the internet. As a result, more industries and professional services have become subject to anti-money laundering (AML) regulation.

Kogan Page's latest book, *Anti-Money Laundering: A Practical Guide to Reducing Organisational Risk* sets out information and guidance on managing the risk of money laundering through analysing regulatory progression; looking at appropriate policies, procedures and training; using an AML 'strategy wheel'; identifying failures of the AML control framework; examining why AML transparency is king on the international stage; due diligence in risk assessment; advantages and disadvantages of weak or strong regulators; and navigating change when implementing AML strategy.

Anti-Money Laundering also includes a number of current and high-profile international case studies to provide readers with a global perspective on the issue and potential remedies.

Author Rose Chapman combines her 20 years' industry experience heading compliance and ethics for global organisations with her academic acumen as a compliance lecturer and a writer for the International Compliance Association to provide a comprehensive guide to effective control methods against money laundering.

" Money laundering is a risk to any organisation engaging in international trade, and it has become a growth industry in recent years – thanks in part to the internet"

This book is written for emerging AML professionals at all levels of an organisation, as well as for those established AML professionals in the regulated sphere seeking to develop an holistic view of the steps their organisation may need to take to better establish AML controls.

News in brief

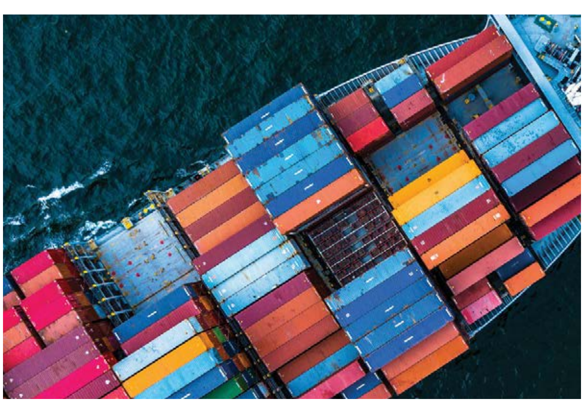
The latest news for business resilience and insurance professionals

The Bank of England, Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) have published a joint discussion paper on an approach to improve the operational resilience of firms and financial market infrastructures. The tripartite group is looking for better standards of operational resilience through increased focus on setting, monitoring and testing specific impact tolerances for key business services which define the amount of disruption that could be tolerated.

Staff at the UK's biggest summer events are being trained in how to react in the event of a terrorist incident, as part of Counter Terrorism Policing's second annual Summer Security campaign. Launched in 2017 in response to attacks in London and Manchester, the programme has delivered advice and training to thousands of festival workers and security guards.

The FCA has published draft rules outlining how it proposes to authorise and supervise claims management companies when it takes over the task in April 2019. Amongst the new requirements are that firms hold capital linked to the type of business they undertake, plus a stipulation that they protect any money held on behalf of clients.

The need for businesses to have a single individual overseeing all aspects of risk is greater than ever, says Airmic. The association acknowledges that not all firms require chief risk officers or their equivalent, but believes complex or very large businesses would nearly all benefit from having one person overseeing risk.



Lloyd's Lab, the insurance market's new innovation sandbox, has launched a global search for tech talent to partner with the Lloyd's market and develop solutions for its unique and rapidly changing needs in this fast-track, fast-fail environment.

Solid underwriting profits have been reported by the UK motor insurance market, with EY's annual market analysis pointing to a net combined ratio for 2017 of 96.8%. This is the best result since 1994 and the second best since records began – and is in stark contrast to the disappointing 109.4% NCR reported in 2016.

The National Cyber Security Centre (NCSC) has published advice for organisations on implementing multi-factor authentication (MFA). It is concerned that uptake of MFA has been slow and, against a backdrop of increasing security threats, this urgently needs to change. The new guidance describes how to use MFA to mitigate against password guessing and theft, including brute force attacks.

Insurers should consider carefully whether current policy limits and sub-limits are appropriate for the reality of new exposures under the General Data Protection Regulation (GDPR), now in force. The International Underwriting Association explores the topic further in a new guide (available on its website), and warns that GDPR raises the possibility of a potential increase in insurance claims for data breaches.

The first blockchain transaction for marine insurance is to be delivered by Willis Towers Watson, along with partners EY, AP Møller-Maersk, XL Catlin, MS Amlin, ACORD and Microsoft. The technology will support more than half a million automated blockchain transactions and help manage risk for more than 1,000 commercial vessels in the first year. By connecting participants in a secure, private network with an accurate, immutable audit trail and services to execute processes, the platform establishes a first of its kind digital insurance value chain.

For more information on these stories and other industry news and views, visit **cirmagazine.com**

A group of insurers, industry bodies and brokers have joined forces to launch an industry-wide programme designed to change behaviours and create "a more inclusive work environment". Led by Lloyd's and Zurich, the Inclusive Behaviours Pledge has attracted the support over 50 firms, demonstrating a commitment to transforming its culture and to driving greater inclusion across the profession.

Organisations are keenly aware of the increasing threat of crises, yet many may overestimate their capabilities to respond. This is among the conclusions of Deloitte's latest crisis management survey, which found that 60% of organisations face more crises today than they did ten years ago.

The commercial insurance sector and its customers must face up to the realities of the fourth industrial revolution if they are to remain relevant. This is the view of Airmic, whose CEO John Ludlow says rapidly changing business models and the advent of digital technologies are creating completely new risk landscapes, creating unprecedented opportunities and challenges for the sector.

Cyber and IT-related risks have been confirmed as the top concerns for Airmic members, according to the association's latest survey. It is also the area where risk managers most want to see the insurance industry extend its offering. Meanwhile, the majority of executives around the world feel their organisations can do better when it comes to learning from past mistakes when it comes to cyber, according to a Willis Towers Watson/Economist Intelligence Unit survey.

Evidence of the impact of climate risk is found across all sectors, geographies, and seasons, according to a study carried out by S&P Global Ratings. The average materiality on earnings for the companies that quantified it is 6%. Publicly-traded companies are becoming increasingly accountable for understanding and mitigating the impact of climate risk.

New technologies could lead to significant improvements in efficiency, including enhanced monitoring, mitigation and management of engineering-related risks. But they bring with them new risks such as cyber. Global engineering insurance premiums for 2017 were estimated at around US$21bn, but have stagnated in recent years, according to the latest sigma study from the Swiss Re Institute.

A worsening of the global trade environment in the coming months, due to a surge in protectionism, could have severe repercussions in Asia-Pacific, according to an Atradius report. Some 45% of the exporters surveyed in the region expect their turnover to decline 10% to 20% due to uncertainty over and changes in trade agreements. These are results of the latest Atradius Asia-Pacific Payment Practices Barometer.

A further surge in data breach and other security failure insurance claims is expected following the arrival of GDPR. A record breaking year in 2017 saw as many cyber claim notifications as for the previous four years combined (which is the equivalent of one for each working day), according to research from AIG Europe.

Identity crisis?

Deborah Ritchie speaks to Andrew Charlesworth about what he believes is a missed opportunity in the government's recently published Biometric Strategy

Andrew Charlesworth is a Reader in IT Law in the School of Law at the University of Bristol, where he is also director of the cross-disciplinary Centre for IT & Law (Law & Computer Science). He currently teaches two masters-level units in the Law School: IT Law and Law of E-commerce; and two undergraduate-level units, IT Law and Privacy Law: Theory and Practice. Charlesworth has taught a masters-level unit, Law and IT, in the Department of Computer Science, and supervises a number of Ph.D. students. His current projects include work on the EU 2020 Horizon project, Privacy Flag. Past projects include working as part of the team that produced the methodology for the conduct of effective Privacy Impact Assessments in the UK and the associated Handbook on PIAs for the Information Commissioner's Office; providing training on addressing cyber crime for police, lawyers and judges in Bulgaria and Romania via the EU Criminal Justice Programme; and EU project work with the City of London Police and UK Finance on 'card not present' crime/internet fraud.

Charlesworth: It's time for some serious debate about biometrics

The Home Office published its long-awaited Biometric Strategy at the end of June. What is your view on the document?
The Home Office's long-delayed Biometric Strategy is, in my view, a missed opportunity for the government to lay out a clear policy and regulatory pathway for the adoption of modern biometric technologies like automated facial recognition (AFR). It is short on detail about the Home Office's future direction for the use of biometrics and the sharing of biometric data, offers no clear statement that facial image databases already deemed illegal will be brought into compliance and lacks recommendations for legislation.

Are there any positive elements contained within the Strategy?
The Biometric Strategy does contain positive measures such as requiring data protection impact assessments for new biometric projects and the creation of a new advisory and oversight committee to advise on policy and standards for AFR. But even here it is disappointing, only promising that "law and standards... [will be] in place to regulate the use of AFR in identification before it is widely adopted for mainstream law enforcement purposes" with little indication of the possible content of such law and standards.

Campaigning groups like Big Brother Watch and Liberty have played a major role in highlighting the biometric policy 'black hole'. Yet they too provide little innovative thinking about how the technology might be regulated. For example, calls for a ban on public sector use of AFR or greater legislative controls ignore private sector use in areas as diverse as site security, marketing, and smart authentication.

We should be wary of a regulatory strategy delivered solely by the blunt instrument of Parliamentary legislation. This might deter investment in development and testing of AFR, with knock-on effects on both the competitiveness of British technology firms and the valuable commercial and social benefits AFR brings to both public and private sectors. Experience suggests it would also fail to adequately address the fairness, transparency and privacy issues that concern campaigning groups.

Are there any pertinent overlaps in the Strategy with other legislation in the UK?
There is already legislation covering the use of CCTV and CCTV analytics, not least the newly invigorated data protection regime brought forward through the General Data Protection Regulation (GDPR). There are also more than enough

> **"Government and industry could work together to develop privacy and data protection standards for architectural regulatory control"**

For better or for worse?

Home Office Biometrics Strategy
This document sets out the overarching framework within which organisations in the Home Office sector will consider and make decisions on the use and development of biometric technology.
gov.uk/government/publications/home-office-biometrics-strategy

EU 2020 Horizon Privacy Flag
The Privacy Flag project has undertaken research to develop the combined potential of crowdsourcing, ICT technologies and legal expertise to protect citizens' privacy when they visit websites, use smartphone applications, or live in a 'smart city'. Its outputs will enable citizens to monitor and control their privacy via user-friendly solutions: a smartphone application, a web browser add-on, and a public website – all connected to a shared knowledge database.
privacyflag.eu

Big Brother Watch response to the Biometrics Strategy
"The government's biometrics strategy is a major disappointment," says director of the organisation, Silkie Carlo. "After five years of waiting, it reads like a late piece of homework with a remarkable lack of any strategy. While Big Brother Watch and others are doing serious work to analyse the rights impact of the growing use of biometrics, the Home Office appears to lack either the will or competence to take the issues seriously. "For a government that is building some of the biggest biometric databases in the world, this is alarming. Meanwhile, the Met today is surveilling Londoners with facial recognition cameras that they have no legal basis to even use. The situation is disastrously out of control. Anyone concerned should support our CrowdJustice campaign to put an end to lawless facial recognition in the courts."
bigbrotherwatch.org.uk

regulators including the Information Commissioner, Surveillance Camera Commissioner (SCC) and Biometric Commissioner (BMC).

Perhaps it is time to turn to other elements of the regulatory toolkit. For some concerns about AFR implementations the most efficient solutions are likely to lie in the technology itself and in better engagement with business and the public in determining its appropriate use and regulation.

Images are often thought of as being more connected to the individual than other forms of personal information. But in terms of analytics they are just another form of data. Control of the use of that data can be integrated into the hardware and software of AFR systems. This approach would provide a verifiable means of achieving practical enforcement of the legal framework. Government and industry could work together to develop privacy and data protection standards for architectural regulatory control, and government could require public sector systems to conform to standards as a minimum, leaving the industry to develop further, more sophisticated controls which could give them a competitive advantage.

> **"Calls for a ban on public sector use of AFR ignore private sector use in areas as diverse as site security, marketing and smart authentication"**

How might some of these issues be more effectively addressed moving forward?
I think it is time for serious debate over the regulation of CCTV analytics like AFR. Both public and industry objectives are poorly served by vague government promises of laws and standards and polarising campaign group rhetoric.

We need to work towards a regulatory framework that provides a proportionate balance between benefits and risks and takes a wider view of the regulatory options available. This should actively encourage CCTV and analytics users to self-regulate through the deployment of appropriate technology architectures and systems.

Interview by Deborah Ritchie

Lethal weapon

- GDPR emails were the bain of our lives in the run up to 25th May but they contributed to a massive increase in awareness of new rules and rights
- Readiness amongst organisations varies wildly, with varying numbers reported in terms of time and money thrown at compliance
- With a real risk of class-action lawsuits in the offing, it may not be the regulator's fines that organisations will fear the most

GDPR Day may be a distant memory, but with the sheer amount of publicity around the EU's new data privacy rules, the real work begins now. As David Adams writes, consumers have found their voice and they're not afraid to use it

Despite a huge number of emails related to the EU's General Data Protection Regulation (GDPR) filling our inboxes during the weeks leading up to the May 25th deadline, the number of people who really understand the EU's latest piece of regulation is probably still very small. Not so insignificant, though, is the subsequent awareness among consumers and employees of their newfound voice over how their data can be used.

In early May, a Veritas survey of 12,500 consumers in 14 countries suggested that more than half would stop buying from a business that failed to protect their data. Six in ten said they would post negative comments about the business online; and three-quarters would report the business to a regulator.

Readers may not be surprised to learn that in the weeks following May 25th, European regulators reported significant upticks in data protection-related complaints.

In effect, risk of regulatory sanction and/or reputational damage following a breach of GDPR terms has added an extra dimension to the data-related risks that organisations of all kinds face, alongside threats posed by attackers or accidental security breaches. These risks will intensify when the EU's ePrivacy Regulation is implemented in 2019.

But while many organisations have clearly put huge time and effort into working towards GDPR compliance, seeking to embed best practice for data management within all its business processes, research from Capgemini published in May suggested that only 55 per cent of UK businesses expected to be largely or completely compliant by the deadline – and this was a higher figure than for businesses in other EU Member States.

Any organisation without a mature risk management process is at a disadvantage when it comes to managing the risks associated with GDPR. Even in highly regulated industries, some businesses are still struggling to complete detailed data audits and to implement new technology and business processes, or to ensure that data storage and processing conducted by third party service providers is also GDPR-compliant.

Mark Thompson, who leads the global privacy advisory practice at KPMG, says there is very little consistency within business sectors when it comes to readiness. "One bank would be OK; another terrible," he says, adding that the largest spend on compliance that they have seen was £200 million (by a global financial services company).

Head of commercial services at Brodies, Grant Campbell, slots companies into three categories of readiness: the largest group, which has created an impression of compliance "but are probably still doing a lot of work in the background"; a second group of organisations that have done most or all of what they need to do; and a third group that are well short of compliance – either because they have taken a calculated risk about how strictly the regulation is likely to be enforced, or because they still do not understand what is required.

For some organisations, outsourcing much or all of the work has been the chosen solution. CRU is a business intelligence provider that specialises in the mining, metal and fertiliser markets and operates from a range of global locations. For several years the organisation has outsourced all its IT security requirements to service provider ThinkMarble, which now also provides it with a virtual data protection officer (DPO) service.

Will Blake, director of technology and analytics at CRU, explains that the company doesn't have the scale to employ a full-time data team internally. Using the ThinkMarble service allows it to access specialist expertise, around the clock, at a relatively low cost. "It takes a great weight off my mind," he says.

The journey towards compliance also requires a re-examination of the legal basis for data processing. Alex Edwards, senior associate at legal firm Rosling King, says one trend in the insurance sector has been a realisation by some companies, as they studied guidance from the ICO, that they were too reliant on 'consent' to justify processing, because explicit consent is more difficult to prove under the GDPR regime. Edwards says there has been a noticeable shift towards greater use of the 'legitimate interest' justification instead.

Weaponising GDPR

It has not taken long for activists to start using GDPR to take the big internet companies to court. On 25th May, Austrian privacy activist Max Schrems filed complaints against Google, Facebook, Instagram and WhatsApp, suggesting that their terms of service violate individuals' rights, as defined by GDPR, to choose how their data is used.

The big technology companies are an obvious target for activists and are also more likely than the average business to attract complaints from individuals. In the past, some businesses may have decided that non-compliance with data protection regulation was a risk worth taking, but GDPR has given the ICO and its equivalent regulators across Europe much stronger powers to punish organisations shown to be non-compliant. How will those powers be used in practice?

In April, the Information Commissioner, Elizabeth Denham, outlined the ICO's intentions in a speech at the Data Protection Practitioners' Conference. She said the ICO would be "as robust as we need to be in upholding the law", without constraining businesses with red tape, "or concern that sanctions will be used disproportionately". Large fines would be reserved for organisations that "persistently, deliberately or negligently flout the law".

Other tools at the ICO's disposal include compulsory data protection audits and enforcement notices. It also has the power to stop an organisation processing data. During May and June it ran a consultation on its regulatory action policy, the results of which will be revealed later in the year.

But the ICO is clearly trying to present itself as a source of support; and it continues to add to the guidance and other resources it provides, including interactive toolkits, sector-specific advice and a dedicated helpline for SMEs.

When the UK leaves the EU in 2019, it will remain aligned with it in data protection regulation terms. But Graham Hunt, director, risk, regulation and compliance at Capgemini, warns that over the longer term there will probably be some divergence between the UK and EU regulatory regimes, driven by differing case law in the two jurisdictions and adding to complexity in trading relationships between entities based in the UK, the EU and elsewhere.

Some businesses based outside the EU have already decided not to serve EU markets until they have clarified possible legal liabilities. Others are seeking GDPR compliance in order to win and retain EU-based customers. In the longer term, Bonner expects GDPR to become a global standard for data protection, matched by similar regulations launched in other countries.

GDPR and the public sector

More than eight in ten UK consumers (83 per cent) are uneasy about sharing data with public sector organisations, according to a February 2018 survey commissioned by IT service provider Proband. Specific concerns were raised about cyber security issues affecting the NHS, HMRC, the DVLA and the police.

GDPR presents a particularly difficult challenge to local councils, which may provide hundreds of different public services. Lynn Wyeth, head of information, governance and risk at Leicester City Council, says that its data audit was a huge task, as was revising the council's data privacy notice. "When you've got 500 services, what granular level of detail do you need?" she asks.

"The public sector has been working pretty solidly on this for a couple of years, with a lot of best practice sharing," she adds, highlighting the council's work with neighbouring councils and initiatives led by the Local Government Association. But, she adds, throughout that time the finances of all public sector organisations have also been constrained by central government policy. It remains to be seen whether austerity will undermine the ability of public sector organisations to comply with GDPR.

There are positive reasons to put a concern for privacy and data protection at the heart of business processes and business models. Campbell suggests that any organisation that makes a virtue of how it handles data will gain a competitive advantage.

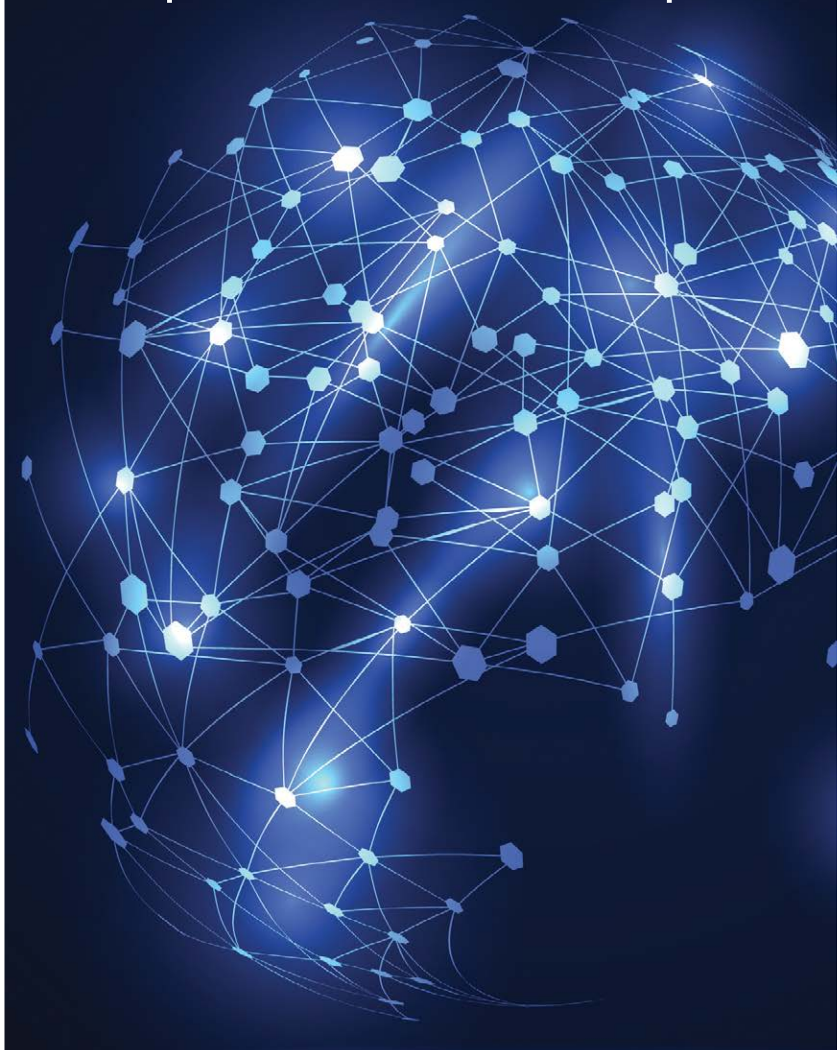
But that theoretically tasty carrot is overshadowed at present by the big stick GDPR has placed in regulators' and consumers' hands. Today, for the many organisations still scrambling to ensure compliance, GDPR is still looking more like a threat than an opportunity.

David Adams is a freelance journalist

Blockchain revolution?

■ It is easy to see how the blockchain can lend itself to the insurance sector. Having one area where data is stored securely (and giving access to those who need it) is one such major benefit.
■ Some believe the technology has the potential to revolutionise the industry. Amongst them Willis Towers Watson, which has just delivered the first blockchain transaction for marine insurance

Much has changed since blockchain was invented just a decade ago. Following the delivery in June of the first blockchain transaction for marine insurance, Angelique Ruzicka explores attitudes towards its wider adoption



When blockchain technology was invented in 2008, few imagined that it would providing anything more than a public ledger of cryptocurrency transactions. But that was a decade ago. Much has changed since then, and even the insurance industry – traditionally considered slow in the adoption of technology – is reaping some of the benefits of the decentralised ledger.

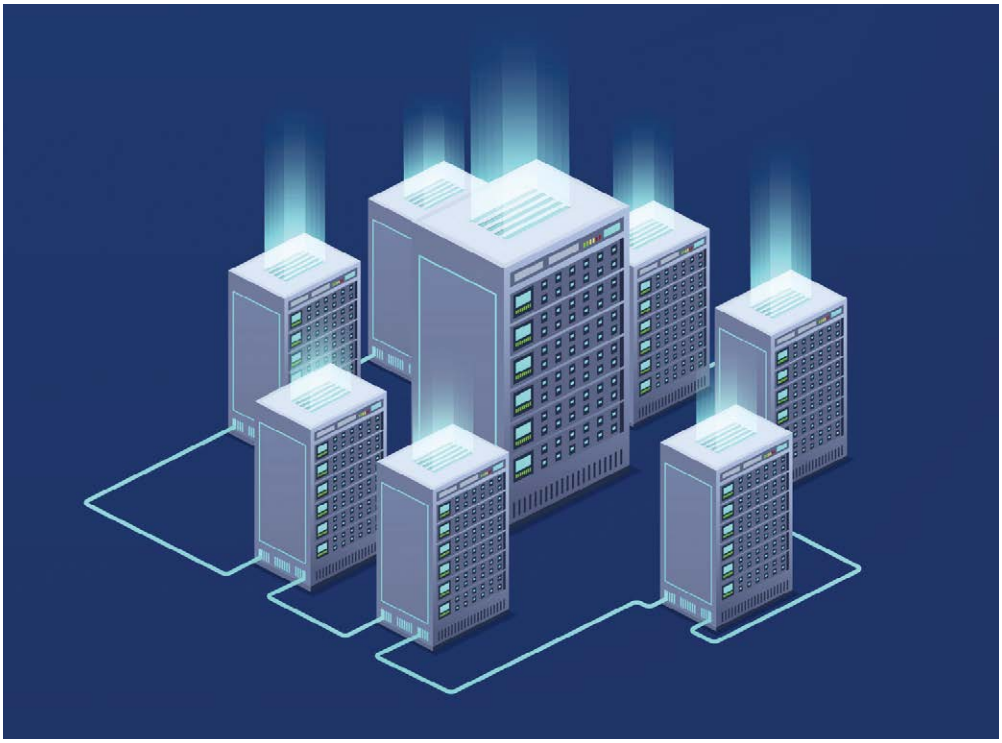
There's something of a shroud of mystery around blockchain, but, by going back to basics, it's easy to see how the technology can lend itself to the insurance sector. Having one area where data is stored securely (and giving access to those who need it) is one such gain.

"Blockchain is essentially an online communication protocol allowing users who are interdependent to participate in a transaction, without any one user having more control over the transaction than the other users," explains UK P&I Club, claims executive, Filip Koscielecki. "All parties to the transaction have access to the same information and no one party can attempt to amend or vary the transaction unilaterally without acquiring the permission of the others.

Sectors set to benefit

Given its heritage, it is somewhat poetic that marine insurance should be the first area to gain traction with blockchain.

In June, Willis Towers announced that it was at the forefront of blockchain technology delivering on the first blockchain transaction for marine insurance along with a consortium of partners, including EY, AP Møller-Maersk, Willis Towers Watson, XL Catlin, MS Amlin, ACORD and Microsoft.



Alistair Swift, head of corporate risk and broking at Willis Towers Watson says the technology has the potential to "revolutionise" the industry. "This is the first insurance transaction that has been undertaken through blockchain, simplifying and streamlining the transactional process and creating added value for our clients," he explains. "We strongly believe this is an industry game changer and that all carriers and brokers should adopt blockchain technology to drive improved transactional efficiency and innovation for their clients."

Head of research and development at law firm Kennedy's, Karim Derrick, agrees. He says that blockchain can help reduce the premiums that shipping companies are paying to insure freight in transit where 40 per cent of the premium comprises transaction costs.

The benefits of keeping complete records – and the avoidance of the consequences of not doing so – are also clear for the sector. "It [shipping] is an immensely huge exercise and a lot of the legal spend occurs when things go wrong and you need to unpick the value chain. But none of this will be necessary when we make use of blockchain," Derrick says.

Other advocates of blockchain say that insurance fraud can be minimised with the use of this technology. Insurance claims can be processed through the use of smart contracts. These contracts would keep a record of vital information such as proof of insurance, claim forms, and material supporting claims. This can all be added to the decentralised ledger by the policyholder making the claim.

Experts say that alerts would be triggered if an individual makes the same claim with another insurer, which could ensure that fraudulent claims are stopped in their tracks sooner and even eradicated.

One insurer has its blockchain ledgers programmed in such a way that the customers don't have to go through the claims process. Last year AXA introduced Fizzy, a completely automated platform that offers direct automatic compensation to policyholders whose flights are delayed. So if a plane is more than two hours late, Fizzy reimburses customers automatically and no brokers or insurance call centre agents are involved.

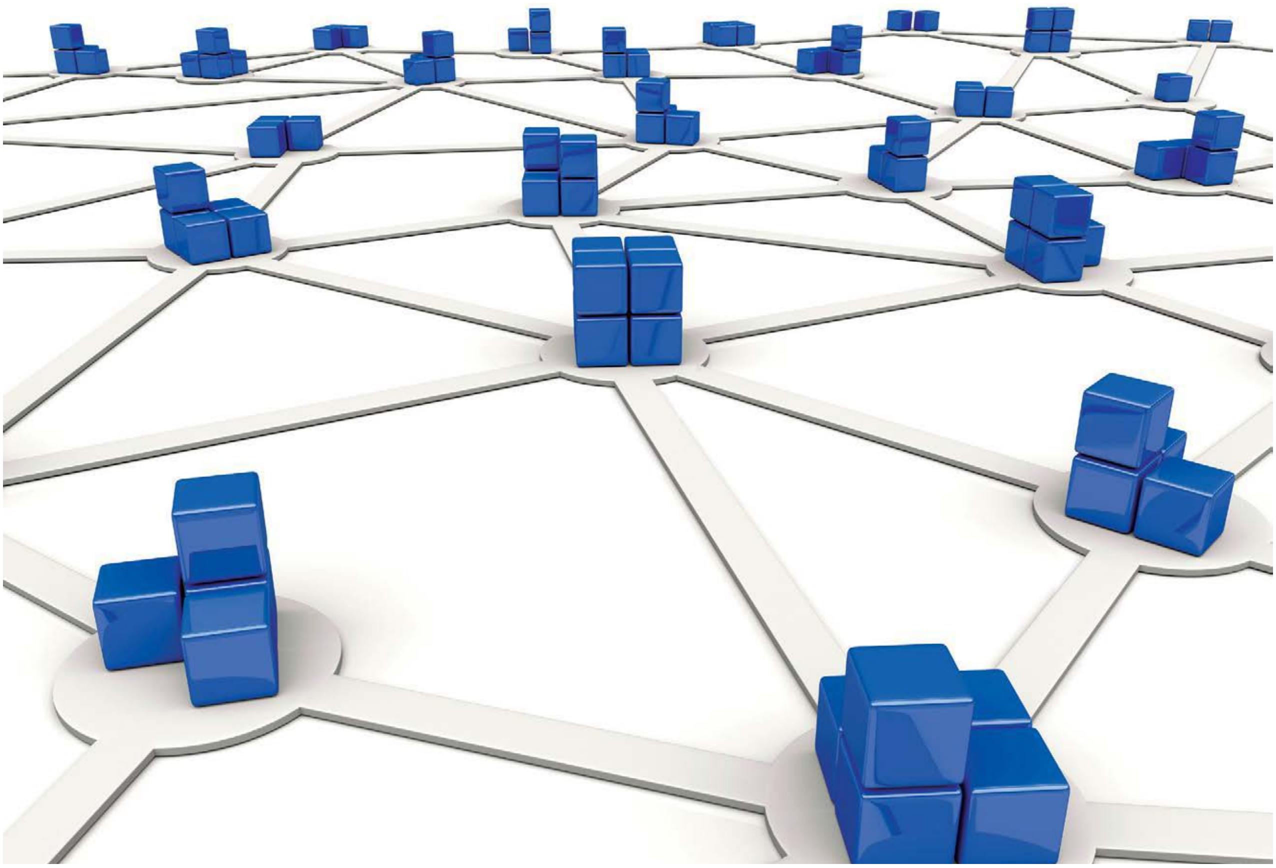
AXA says this is all possible through the recording of the flight purchase in its tamper-proof network, the Ethereum Blockchain. This smart contract is then connected to global air traffic databases, which then triggers compensation in the event of delays.

Legal and regulatory concerns

Blockchain can offer numerous benefits but, ironically, it is one of these very advantages – the ability to record data without it being altered or tampered with – that could prevent it from being fully embraced.

With the industry seeking to ensure that it's compliant with General Data Protection Regulation (GDPR), blockchain technology clashes with consumers' rights to 'be forgotten'.

"On a traditional blockchain all transactions are permanently recorded, so there is an incompatibility there. Also, for insurance in particular, policy documents need to be stored. These are often quite large legal documents, which would take up a lot of room



on the blockchain and slow down the transaction processing," points out CEO at Tapoly, Janthana Kaenprakhamroy.

Some blockchain providers say they can work around these issues by only storing references on the blockchain, which point to other data stored outside of it. "However, in that case you are not getting the security and other benefits of the blockchain for that external data, so it could still be altered post-transaction which defeats the point of using blockchain in the first place," she says.

When security breaches occur, companies are under an obligation to report the matter to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it and affected individuals must also be informed. While many claim that blockchain is secure, it is not hack-proof.

"Blockchain can offer numerous benefits but, ironically, it is one of these very advantages – the ability to record data without it being altered or tampered with – that could prevent it from being fully embraced"

Despite legal concerns, blockchain is expected to form an integral part of our world in the future.

"The predicted overall impact of blockchain and smart contracts on trade is significant. The World Economic Forum estimates that 10 per cent of GDP will be stored on blockchain by 2027," P&I's Koscielecki points out.

"Regarding security, there have been some cases, particularly for virtual currencies, where the blockchain has been manipulated by hackers. Defenders of blockchain will point out that these attacks were usually targeting bugs in the code and that blockchain itself is a secure concept, but still it shows that the technology has some way to go before it is mature enough to use on a daily basis," Kaenprakhamroy explains.

She says it's these sorts of issues that represent the greatest barrier to adoption in the insurance industry. "If blockchain could be made GDPR compliant, if the cost was lower, and if the performance was up to our standards, then of course we should adopt this technology, but until these issues are addressed I expect most InsurTech or FinTech companies will hold back and wait," she says.

Angelique Ruzicka is a freelance journalist

A new chapter

▪ The confidence that returned to the manufacturing sector following the financial crisis has waned slightly amid ongoing Brexit uncertainty
▪ Despite this, some UK businesses are already trading actively beyond the EU, with more forecast, with electronics continuing to do well
▪ Some commentators believe there may be good reason to believe that manufacturing will continue to represent around 10% of the British economy

The slow post-war decline of the UK's manufacturing sector was showing signs of stabilising, but uncertainty surrounding Brexit negotiations has led to a wobble in the sector. Graham Buck spoke to the industry about its prospects

Ten years on from the global financial crisis, the UK's manufacturing sector is undoubtedly leaner, but is it any meaner? A GMB union report shows that in 2007, the UK supported 3.5m permanent and temporary manufacturing jobs – more than 12 per cent of British employment. In 2016 those figures had declined to 2.9m and 9.2 per cent respectively.

"Uncertainty [surrounding] the government's approach to Brexit is harming UK manufacturing and delaying important business investment decisions that will provide high quality jobs in the years to come," says GMB national secretary, Jude Brimble.

The report was just days old when Rolls-Royce announced job cuts of 4,600 jobs worldwide – 3,000 of which from its UK operations. Meanwhile, Airbus warned that the ongoing dithering with Brexit negotiations meant it was reviewing the future of its British operations. The Society of Motor Manufacturers (SMMT) added to the pressure on the government, reporting investment in the UK automotive industry in the first half of 2018 slumped to £347m, from £647m in the same period in 2017.

While sterling's weakness in the two years since the EU referendum has shored up manufacturing activity and export order books, some recent data suggests it's only a temporary benefit. After last winter's Beast from the East disrupted business, an anticipated recovery in April failed to materialise; output fell by 1.4 per cent.

Employers are also alarmed by the impact of Brexit uncertainty on manufacturing investment. Last month the Confederation of British Industry's (CBI) outgoing president, Paul Drechsler, warned: "If we do not have a customs union, there are sectors of manufacturing society in the UK which risk becoming extinct."

He added that "hundreds of millions" had been diverted by

Photo by: Rolls-Royce plc

Britain's pharmaceutical and finance companies into ensuring business continuity should a potential 'worst-case' post-Brexit scenario becomes a reality.

To offset the gloom, the CBI's most recent industrial trends survey offers more upbeat news. Manufacturers reported healthier order books in Q2, exports remained well above average while the majority of sectors recorded growth, led by mechanical engineering and food, drink and tobacco.

Tom Hunt, underwriting manager for QBE's European operations, suggests that a weak pound hasn't been the only contributory factor. "Relatively buoyant conditions for UK manufacturing since the 2016 referendum have correlated with those for manufacturers across the EU and numerous countries worldwide," he reports. "To some extent, therefore, a case can be made that favourable conditions seen in the UK also required similar conditions to exist within the EU – our closest trading partner – and worldwide.

"Moreover, the UK's core downstream industries such as construction, automotive, aerospace and infrastructure have provided a stable and predictable flow of orders in recent years meaning capacity has been utilised to higher levels and manufacturers have been able to invest in plant/efficiencies and – to some extent – forecast more accurately. Much of this may be about to change however."

An emerging threat comes from the US-China trade dispute that threatens to escalate from tit-for-tat to all-out war could easily bring that progress to a halt. The vulnerability of the UK's remaining steel industry to tariffs on European producers has already underlined the potential collateral damage.

Meanwhile, business banking market researcher East & Partners reports that UK businesses are seeking trade with new markets beyond Europe, evidenced by their reduced use of the euro for international trade this year. The decline, along with small increases in their use of the US dollar and Chinese renminbi contrasted with a sharp rise in the use of other currencies, which rose nearly 25 per cent.

"While uncertainty continues with Brexit negotiations, UK business isn't waiting and is already trading more [actively] beyond the EU," said Simon Kleine, East and Partners Europe business lead. "Their usage and forecasts of currencies, as we head towards 2019, show they are starting to trade more widely and are looking to increase it."

Germany's example

UK manufacturers' association the EEF – formerly the Engineering Employers' Federation – also offered more reassuring news in its Q2 Manufacturing Outlook, produced with BDO. Although recruitment and investment plans have eased since 2017, they remain positive.

"Producers of mechanical equipment and electronics continue to do well and many companies are reporting strong demand from overseas," reports Francesco Arcangeli, an economist at EEF. Before Airbus' recent warning, the outlook for aerospace was also looking good.

"It's impossible for the UK to go back to the position of 30–40 years ago, or for the country to match Germany, but there's good reason to believe that manufacturing will continue to represent around 10 per cent of the British economy and this figure is stabilising."

Arcangeli suggests the methodology in the GMB report was "a little flawed".

"There has indeed been a loss of manufacturing jobs in the past decade, but the majority occurred in the two years after the 2008 crisis. Since then the trend has been a flatlining rather than decline and in the past year has been much improved – a point that most reports overlooked."

UK manufacturing has nonetheless felt pressure from emerging economies and the shift of many manufacturing activities to lower-cost locations, says Tom Lawton, national head of manufacturing at accountancy and

business advisory firm BDO, who notes that China, in turn, is now being undercut by cheaper competitors. "Although British manufacturers have tended to look closer to home, many opting to transfer production to Eastern Europe rather than Asia, as evidenced by Jaguar Land Rover's decision to move work from the West Midlands to Slovakia," he adds.

Lawton notes that Germany offers an example close to home of a highly successful manufacturing economy, helped by its Fraunhofer network of technical institutes that unite researchers and manufacturers. It's an idea that Britain has aimed to replicate via the network of Catapult centres established by Innovate UK.

"Unfortunately we haven't been as good as Germany in developing long-term planning and industrial strategy that works to a programme of 20 years or more," he says. "Theresa May made some terrific pronouncements on industrial policy on entering Downing Street, but her attention has understandably since been diverted.

"In addition, feedback suggests that with the advent of the fourth industrial revolution – aka Industry 4.0 – our skills shortage is particularly acute as suitably qualified individuals will be needed within just five years."

However, Sjaak Schouteren, a partner within the European cyber team at JLT Specialty, is hopeful that industry can rise to the challenge and has already seen much innovation within manufacturing.

"Where these companies used to run on operational technologies like supervisory control and data acquisition (SCADA), industrial control systems (ICS) or distributed control system (DCS), they are now looking at how to safely incorporate the industrial Internet of Things (IoT).

"We see a lot of organisations boosting their growth and success using connected devices and integration; by combining the manufacturing process with their need to drive data into every component of the organisation. Manufacturing companies are looking increasingly at the benefits of IT/OT integration and the industrial IoT. They continue to connect networks that operate at very different levels and means of security."

Supply chain focus

Brexit uncertainties have focused attention on tackling supply chain risk, which was already steadily moving up the agenda for manufacturers, says Simon Gallimore, manufacturing industry UK lead for AIG.

"While the needle is moving in the right direction in terms of awareness, there's still some way to go," he reports. "In our work with manufacturers over the years, we have found that the many do not have a clear understanding of their supply chains, nor an enterprise-wide approach to managing these risks.

"Unfortunately, there's no silver bullet to guarantee business continuity. Until recently there has been a limited ability in the market to properly quantify supply chain risks and subsequent contingent business interruption due to a lack of tools and processes both in the insurance industry and on the client side."

The weakness of the post-Brexit pound has also proved to be a double-edged sword for the food and drink manufacturing sector, currently hit by production difficulties caused by northern Europe's most acute shortage of carbon dioxide (CO_2) in 40 years. Supplies of the gas, used in everything from food packaging to putting the fizz in drinks to food packaging, arose as several plants closed for maintenance just as demand was escalating.

Darren Seward, sector lead for hospitality and food/drink at NFU Mutual, says Brexit has pushed up the price of imported goods, often forcing food and drink manufacturers to improve supply efficiencies, reduce margins or increase their own prices in efforts to maintain quality. "In attempts to offset rising import costs, the industry is sourcing more goods produced in Britain," says Seward, which he regards as a "huge opportunity" for British craft breweries, distilleries and even vineyards.

Graham Buck is a freelance journalist

- The means and perpetrators of terrorist attacks has changed greatly in recent years, with attacks by lone wolves or small groups on the increase
- Some changes are leaving the traditional property-based insurance market behind. bringing the issue of physical damage to property to the fore
- In addition to introducing BI extensions, many insurers are looking at their lone attacker definitions and rethinking liability related to vehicles

Closing the gap

The evolving terrorist threat has led to significant shifts in risk managers' needs when it comes to insurance. Ant Gould examines the new dynamics and looks at how the insurance industry has responded to calls for change

Former British prime minister, Harold Macmillan once said the most difficult thing about planning is "events, dear boy, events" and in the UK alone, terrorist attacks including Westminster, London Bridge/Borough Market and the Manchester Arena have certainly resulted in a major change in the threat to risk managers – from being bombed out of their premises to being kept out of them.

As deputy CEO and technical director at Airmic, Julia Graham, puts it, "the means and perpetrators of attacks has changed. Attacks by lone wolves and small groups against perceived soft targets has increased; the use of vehicles as weapons has increased; and the threat of cyber attack continues to grow."

Graham's view is echoed by both Marsh's 'Terrorism Risk Insurance Report' and Aon's 'Terrorism and Political Violence Risk Map' – the latter pointing to yet more bad news to come. "A deterioration in governance around the world gives space to terrorist groups to sustain their operations and create the opportunity for terrorist groups to reach out and impact populations and businesses at an immediate, tactical level across the world," it reads.

The changing impact is leaving the traditional property-based insurance market behind. Last year's attack in London Bridge, for instance, caused an estimated £1.4m of economic losses, as stallholders and restaurants were forced to close for almost two weeks. But because the terrorists did not cause any major physical damage to the affected businesses' properties, Pool Re – the UK's state-backed reinsurer – did not pay out after the incident.

In fact, the only incident that Pool Re did pay out for last year was the Manchester Arena bombing in May, which caused physical damage to a number of buildings.

Meanwhile, the poisoning of Sergei and Yulia Skripal in March – further highlights insurance gap issues; the Salisbury incident showed the potential impact of a relatively small amount of nerve agent, with a clean-up operation spanning over 27 miles. Businesses were affected by the event for months – and not just those inside the police cordon; the wider retail and tourist industry impact is thought to equate to a 50 per cent decrease in footfall.

The Salisbury incident and London Bridge attack both highlight the issue with Pool Re – and other state-backed terrorism reinsurance schemes – that only business interruption (BI) caused by property

Photo by: Amani A / Shutterstock.com

damage is covered. After extensive lobbying by Pool Re this is about to change and the government is seeking to amend the Reinsurance (Acts of Terrorism) Act 1993 via the Counter-Terrorism and Border Security Bill. Introduced to the House of Commons in June it will extend Pool Re's cover to include terrorism related non-damage BI losses, and, if passed, Pool Re will be the first terrorism insurance pool in the world to extend its cover in this way.

Chief underwriting officer at Pool Re, Steve Coates says: "We are currently working on our proposition and talking to key scheme stakeholders to ensure it integrates with member BI policies. As with our damage cover, the financial limits will reflect those on the underlying non-damage BI cover within the member's property/BI policy. Timing is subject to the successful passage of the amendments to the Act of Parliament, but we are aiming for early 2019. We are hopeful this amendment will encourage more businesses to buy terrorism coverage, especially SMEs – many of whom do not [currently] buy any terrorism cover."

The emphasis on encouraging SMEs to take out cover is a continuing theme for Pool Re. The British Insurance Brokers Association estimates that only three per cent of SMEs have terrorism cover of some sort, despite Pool Re's decision last autumn to half the cost to insurers for some types of small business cover.

Managing director of crisis management at Gallagher, Paul Bassett, says the situation in the mid to large corporate market is very different. "We see several hundred risks a year and believe the majority of mid to large corporates based in the UK buy some [form of] terrorism related [cover] – I would say 80 to 90 per cent have. Risk managers really

need to understand and analyse their coverage carefully – neither the Pool Re or standalone market solutions are perfect, but there have been many changes and movement in the last two years."

Will the change to Pool Re make any difference to the overall market, given how much cover outside of the pool purports to cover non-damage BI? An Association of British Insurers spokesman says "while there is a market for non-damage BI, this change should hopefully [encourage] more widespread coverage. The impact of this may also depend on how the legislation applies in practice."

This 'the devil will be in the detail' response is echoed around the market, but most expect to see more non-property based BI cover emerging, which, as Airmic's Graham implies, will be lapped up if the price and coverage is right. "Insurers typically have not developed non-damage BI covers – although the demand is there," she says.

New threat, new response

Outside of the BI extension, the market is responding to events in a number of other ways. Many insurers are looking at their lone attacker definitions – often involving a hand-held weapon, including knives, guns and explosive devices. One such insurer is Hiscox, which has created a Malicious Attack policy that provides cover whether an attack is the work of a terrorist or a disgruntled employee including loss of attraction cover within a one-mile radius of an attack.

Insurers are also rethinking liability related to vehicles and

CBRN

CBRN (chemical, biological, radiological, nuclear) has historically been excluded from all commercial property and BI insurance policies as it was thought the sheer magnitude of the potential losses would exceed the ability of insurance and reinsurance companies to meet claims. However, the Salisbury incident shows that these types of attack can be localised.

Pool Re provides cover for CBRN but only when a physical damage trigger – but that will change as Pool Re's Coates says: "Pool Re has covered CBRN since 2003. Damage caused by CBRN means will be covered and there is no exclusion of contamination as would be found in a property policy. Once our coverage extends to non-damage BI, this would also include such things as denial of access due to a CBRN peril that does not cause damage to property."

Cyber terrorism

Pool Re has added cyber terror to cover material damage and direct business interruption (BI) caused by acts of terrorism using remote digital interference.

Pool Re's Coates says: "Cover was made available from 1st April this year and the response has been extremely positive. This future proofs the scheme against a threat that may emerge in the future. Terrorists clearly have cyber skills, but they are not yet sophisticated enough to cause damage by remote means, but that could change.

"Our reinsurance charge to the market was not increased to reflect the wider cover as the member retentions were increased at the same time, and the price to policyholders is decided by the insurer. We do not cover war and it was felt that acts of organisations controlled by nation states should be treated in the same way."

And therein lies the rub as it is very challenging to attribute cyber-attacks to a certain actor. As Gallagher's Bassett observes most of the few relevant events there have been so far were probably state-sponsored. He adds: "There is also a perception with buyers that Pool Re covers data and money –but it doesn't, and they are excluded from Pool Re. It is best" he says, "to go to wider specialist cyber market to get the right cover".

expanding the definition of a hand-held weapon. Insurer XL Catlin has this summer launched its Auto Terror Protect offering for fleet operators, vehicle rental, haulage and logistics companies providing cover for third parties and employees who may be injured in a terrorist attack, as well as first-party property damage for the vehicle and any goods in transit.

The Motor Insurers' Bureau is also polling its insurer members on whether the industry pool for uninsured motor claims should re-assume liability for claims arising from terrorist attacks using vehicles. The vote requires 75 per cent of members to approve for the changes to be passed.

Outside of pure insurance coverage, there is a flourishing market for risk prevention and response services – an area that the Marsh 2018 report suggests could be one of the major areas of growth over the next two years – and risk managers can expect a raft of revised and new offerings from insurers, brokers and third parties in this area over the coming 12 months.

In the final analysis, as terrorism attacks change, and insurance evolves in response, there should be more choice and more affordable and relevant coverage available for risk managers. However, inevitably the proof will be in the pudding when it comes to claims as to whether the market has really understood the risk it is starting to take on.

Photo by: Brian Minkoff / Shutterstock.com

Ant Gould is a freelance journalist

20th ANNIVERSARY

BUSINESS CONTINUITY AWARDS 2018

Twenty years of celebrating excellence in business continuity, security and resilience

WINNERS' REVIEW

cirmagazine.com/businesscontinuityawards

In association with

CITY OF LONDON

Main award sponsor

SUNGARD AVAILABILITY SERVICES

Sponsors

BARCLAYS

Business Continuity Transport

clearview Making the Complicated Simple

daisy

Fortress

FUSION RISK MANAGEMENT

PlanB Consulting

Sentinel

The Retailers Business Continuity Association

Supporters

airmic

alarm

SCOTTISH CONTINUITY

20th ANNIVERSARY BUSINESS CONTINUITY AWARDS 2018

Congratulations to this year's worthy winners...

Best Contribution to Continuity and Resilience Sponsored by YUDU
WINNER: Barclays

Global Award
WINNER: Dubai Airports Corporation

DRaaS Award
WINNER: Water Direct

Cloud based Services
WINNER: Zerto

Most Innovative Product of the Year Sponsored by the Retailers' Business Continuity Association
WINNER: citizenAID

BCM Planning Software of the Year
WINNER: Daisy Shadow Planner

Excellence in BC in Industry Sponsored by Plan B Consulting
WINNER: HomeServe & Daisy

Excellence in BC in the Financial Sector Sponsored by Daisy
WINNER: Barclays

Transformation Award Sponsored by Barclays
WINNER: DVLA
Highly commended: RSA

Incident Management Award Sponsored by Clearview
WINNER: USAA
Highly commended:Imperial College London

Initiative of the Year sponsored by CMAC Business Continuity Transport
WINNER: Marks & Spencer

Strategy in Partnership
WINNER: Civil Nuclear Constabulary & CMAC Business Continuity Transport

Strategy of the Year sponsored by Sungard Availability Services
WINNER: Lloyds Banking Group

Most Effective Recovery of the Year sponsored by Fortress
WINNER: CITI

Specialist Technology Company of the Year
WINNER: FireEye

Specialist Company of the Year
WINNER: CMAC Business Continuity Transport
Highly commended: International SOS

Team of the Year Sponsored by Daisy
WINNER: RSA
Highly commended: DVLA

Adviser of the Year
WINNER: Ewan Donald, PlanB Consulting

Newcomer of the Year
WINNER: Amelia Barton, Regester Larkin by Deloitte

Lifetime Achievement Sponsored by Fusion Risk Management
WINNER: Steve Mellish, Mellish Risk & Resilience

Manager of the Year Sponsored by Sungard Availability Services
WINNER: Nicky Russell, RBS

Ambassador Award
WINNER: Sungard Availability Services

Incident Management Award

Bal Chhokar, manager, Member Solutions, USAA; Maurice Williams, executive director, Business Continuation, USAA; pictured with Ian Crabb, CEO, ClearView Continuity; and host Paul McCaffrey

Winner USAA

The judges said: The intensity of Hurricanes Harvey and Irma robustly tested USAA's incident management capabilities, and this year's panel of judges were humbled by this winning entry

About: Hurricanes Harvey and Irma delivered a crippling blow to the southern US in 2017. It was the first time on record that two Category four landfalls occurred in the US in the same hurricane season, much less within 16 days of each other. Harvey is expected to be the most expensive natural disaster in US history. Damages are expected to exceed US$160bn. Irma prompted the largest evacuation order in US history as nearly 6.4m people were ordered to evacuate or seek shelter.

USAA's Unified Command Centre recognised the threat posed by both storms long before they made landfall and executed action plans to proactively mobilise teams and resources to safeguard over 23,000 employees at 19 facilities in the paths of the two storms. These plans included closing the company's headquarters for Harvey, closing its Tampa Regional Offices and ceasing all operations in Florida for Irma; requiring a massive employee accountability process. As the storms formed, an interactive web map was created for each hurricane, with live weather feeds updated near-real time, personnel locations (updated daily), third party suppliers' capabilities (updated every 30 minutes) and operational locations (daily).

"Our corporate comms team launched an information campaign which included tactics such as: member comms, leadership comms, claims reporting resources, alerts on usaa.com, and an event specific webpage providing on-site location information," said executive director, Business Continuation at USAA, Maurice Williams. "External comms included public relations outreach, social marketing, paid search, online and radio advertisements. Internal comms included leadership, as well as digital billboards to promote employee safety and campus closure information.

"Due to the severity of the storms, anticipated impact on employees and their availability for work, USAA stood up an Agile Response Team to respond to employee needs with greater agility, speed and clear accountability. This approach kept USAA ahead of the curve, allowing for appropriate planning for employees and their families and enabling USAA to successfully maintain its ability to serve its members before, during, and after the hurricanes."

usaa.com

USAA®

20th ANNIVERSARY
WINNER
BUSINESS CONTINUITY AWARDS 2018
INCIDENT MANAGEMENT AWARD

Best Contribution to Continuity and Resilience

Richard Green, vice-president, Incident & Crisis Management, Group Resilience, Barclays; pictured with Richard Stephenson, CEO, YUDU Sentinel and host Paul McCaffrey

Winner Barclays

The judges said: Barclays has shown its commitment to helping small to medium sized enterprises with their own resilience efforts, mirroring its dedication in this arena.

About: Small and medium-sized enterprises are key drivers of economic growth, and account for 48% of private sector employment in the United Kingdom. Many of these organisations show tremendous potential for growth, with annual revenue growth rates at or above 25%.

Disruptive events can happen anywhere and at any time, and helping small business owners to create resilience and build recovery plans helps to guarantee their future prosperity, as well as that of the UK.

It has never been so important for UK businesses to help SMEs be more resilient, so in 2017, the Group Resilience team at Barclays rolled out a series of impactful and diverse events as part of its BResilient campaign targeting specific SME customers and audiences across the country in order to promote, explore and embed a culture of resilience within the mindset of small business owners.

From direct relationships with businesses to digital tutorials, the team has been able to capture the imagination of the SME community, engaging and informing them through scenarios with the use of virtual reality technology.

"Barclays is committed to supporting communities in an holistic and tangible way, sharing skills and knowledge as well as promoting a new way of thinking to consider risks, up skill SMEs and promote a resilience way of thinking," says Lee Webb, director, Group Resilience at Barclays.

"Partnering with Business in the Community, Barclays Digital Eagles, In Your Face Advertising and Vivida, the aim is to increase resilience awareness in the wider community and enable businesses to be better prepared for events which have the potential to disrupt their business through initiatives such as the #BResilient campaign via a number of events.

"Participants were taken on a journey using VR technology through scenarios which drew on the catastrophic impacts of not being resilient in an engaging and informative way."

barclays.co.uk

BARCLAYS

20th ANNIVERSARY
WINNER
BUSINESS CONTINUITY AWARDS 2018
BEST CONTRIBUTION TO CONTINUITY AND RESILIENCE

Excellence in BC in the Financial Sector

Sean Deadman, vice-president and UK Resilience Partner, Barclays; pictured with Andy Dunn, head of availability services at Daisy Group and host Paul McCaffrey

Winner Barclays

The judges said: Barclays puts the most important stakeholder, the customer, at the heart of its resilience approach

About: The financial sector faces many unique challenges, amongst them the financial services regulatory regime and an ongoing legacy of consumer mistrust following the 2008 financial crash. An environment of change, including digital transformation, growth of the sharing economy, the advent of crypto currencies, challenger banks, increasing customer expectations and high levels of scrutiny all make operating in the financial sector a greater challenge today than ever before. Addressing these issues is vital, and Barclays has shown a commitment to rebuilding trust in its brand and in the banking community as a whole. It has achieved this in part by embedding a resilience ethos at all levels of the organisation.With the support of a committed resilience team and new technologies, the last 18 months have seen Barclays achieve much of its planned transformation; and it has clearly identified the next steps for successful completion.

"Resilience by Design was the concept introduced to ensure resilience is not an afterthought competing for management attention but is on the board agenda and an integral part of the way the firm assesses, measures, evaluates and responds to risk," says Mike Butler, managing director, Group Resilience at Barclays.

"Enterprise risk themes were introduced into the overall Risk Framework to drive action and improvements with a series of videos produced to help explain the concept of resilience to colleagues. A further initiative to better prepare for disaster and increase resilience capabilities was the Near Miss function which educates and delivers cultural change by changing the way risk is perceived and countered.

"Having seen the value of Near Miss internally and wanting to positively influence the industry, Barclays established an independent Global Near Miss Cross-Industry Forum to leverage experience from a variety of different industries to share best practice and align strategies on joint risks. Forum members include Sungard Availability Services, Sky, BA, Tesco and Colt Telecoms. As a good corporate citizen, Barclays promotes the importance of resilience to the wider community. Initiatives such as the widely advertised 'Digital Eagles', present in branches to build customers' internet skills, and the #BResilient campaign in conjunction with Business in the Community to promote the resilience message to SMEs are part of this strategy."

barclays.co.uk

BARCLAYS

20th ANNIVERSARY
WINNER
BUSINESS CONTINUITY AWARDS 2018
EXCELLENCE IN BC IN THE FINANCIAL SECTOR

Strategy in Partnership

The winning teams at the Civil Nuclear Constabulary and CMAC BCT, pictured with Jane O'Leary, Alarn and awards host Paul McCaffrey

Winner Civil Nuclear Constabulary & CMAC Business Continuity Transport (BCT)

The judges said: The Civil Nuclear Constabulary & CMAC BCT work together to transport and accommodate police officers in times of national emergency, through a bespoke plan that covers all areas of the UK. This partnership was recently called upon after the terrorist attack at the Manchester Arena and the failed attempt at Parsons Green.

About: CMAC Business Continuity Transport works with the Civil Nuclear Constabulary (CNC) to provide transport and accommodation to police officers in times of national emergency, covering isolated locations across the UK to move armed police officers once mobilised.

This partnership is part of the counter terror plan known as Operation Temperer. CNC's contribution involves the no-notice mobilisation of over 400 armed officers from locations across the UK. Since its inception, CMAC BCT have been involved in the development and testing of the CNC element of this national plan. We have worked closely with the CNC to create a bespoke plan for emergency transport and we have helped refine the response time from days to a matter of hours.

"We work by providing the CNC with live inventory of transport and accommodation services across the UK giving us the ability to relocate instantly once invoked. The solution allows the CNC to have little or no impact on their recovery plans whilst also allowing them the freedom to continue with their task in hand of reducing the UK's terror threat level," said Steve Turner, CEO at CMAC. "Central to our operation is ensuring availability of transport and accommodation. This is done on a daily basis using our bespoke software system which provides full visibility of available transport on our UK network, to ensure that we have the ability to deliver against multiple invocations across locations should we need to."

Chief Constable Mike Griffiths said, "With the intimate support of CMAC we deployed at very short notice over 800 officers across two deployments to 23 different Home Office force areas in a matter of hours. The critical element in the success of this deployment was the hard work and detailed planning which went into this contingency plan and the close working relationship we have with CMAC. They understood our needs and delivered our people to the locations from which they were able to conduct their armed policing tasks. This was truly a joint endeavour."

cmacgroup.co.uk/businesscontinuitytransport

CIVIL NUCLEAR CONSTABULARY

CMAC Business Continuity TRANSPORT

20th ANNIVERSARY

WINNER
BUSINESS CONTINUITY AWARDS 2018
STRATEGY IN PARTNERSHIP

Specialist Company of the Year

The winning team at CMAC BCT; pictured with awards judge and head of business continuity for UK&I, EMEA & APAC at Experian, Dean Beaumont; and awards host Paul McCaffrey

Winner CMAC Business Continuity Transport (BCT)

The judges said: In a closely fought category, this impressive outfit has done it again. There is something very different about CMAC and the services they offer. They are always on the scene quickly. They've even gone as far to to make arrangements with first responders. On top of this, countless customer testimonials vouch for their excellent service.

About: CMAC BCT is a leading UK dedicated provider of emergency and pre-planned managed transport services. CMAC BCT offers clients a UK network of over 4,000 approved and compliant ground transport operators; constant monitoring of vehicle availability via unique system software technology; emergency hotel accommodation and marshalling; and a UK-based control centre handling calls 24/7/365. CMAC BCT currently has over 100 employees who handle invocations, tests and queries from over 100 contracts. In 2017, the company managed the movement of over 1,000,000 people in emergency situations. CMAC BCT works with each client to create a bespoke plan for the evacuation and transport, and if necessary accommodation, of employees and customers in the event of an invocation. For an office-based business this may mean moving employees to and from their homes, mainline or tube stations, or designated pick-up points to a recovery site, until permanent accommodation is restored. For airlines, which are an important part of the company's business, it may involve providing marshals and accommodation in addition to transport for their customers. When invocation occurs, the situation is not always what was planned for. Although planning is crucial, experience has shown that it is also essential to be flexible and able to respond changing requirements.

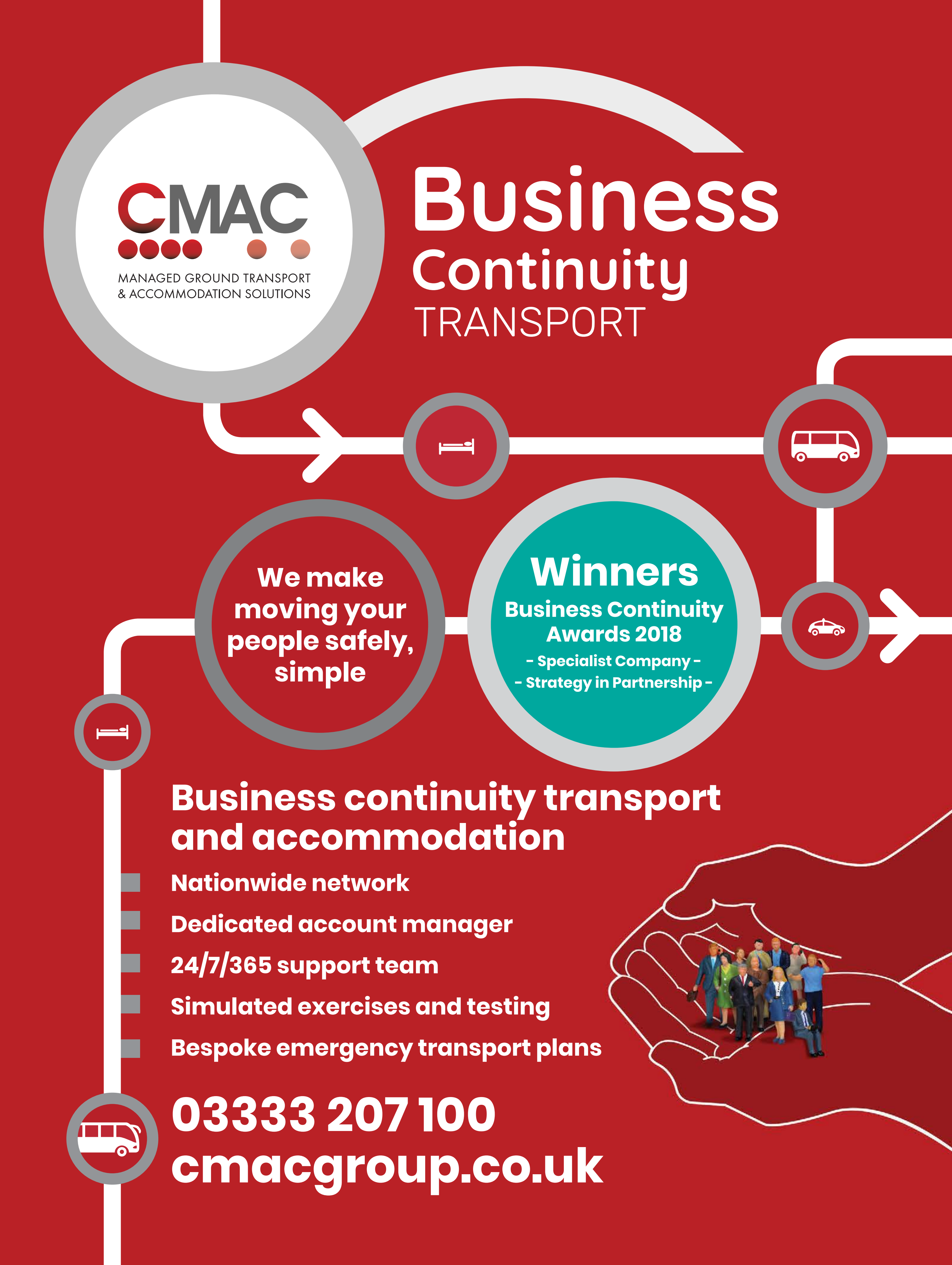
On 2nd October 2017, CMAC BCT received a call from its client, the Civil Aviation Authority, to activate contingency plans and assist in the repatriation of Monarch Airline customers. Over a three-week period, the company assisted in what became the biggest ever peacetime repatriation exercise. Over 32,000 passengers were moved by CMAC BCT and its suppliers during this time.

"This was one or our busiest periods since CMAC began operations ten years ago," said chief operating officer at CMAC, Peter Slater. "It was a pleasure to help support the CAA during this time and I am very proud of how professional all the teams involved from CMAC and the CAA were and how well we worked together during what was a very stressful time."

cmacgroup.co.uk/businesscontinuitytransport

CMAC Business Continuity TRANSPORT

20th ANNIVERSARY
WINNER
BUSINESS CONTINUITY AWARDS 2018
SPECIALIST COMPANY OF THE YEAR


CMAC
MANAGED GROUND TRANSPORT
& ACCOMMODATION SOLUTIONS
Business
Continuity
TRANSPORT
We make moving your people safely, simple
Winners
Business Continuity Awards 2018
- Specialist Company -
- Strategy in Partnership -
Business continuity transport and accommodation
Nationwide network
Dedicated account manager
24/7/365 support team
Simulated exercises and testing
Bespoke emergency transport plans
03333 207 100
cmacgroup.co.uk

BCM Planning Software of the Year

Colin Jeffs, head of business continuity management, Daisy Group; pictured with Charlie Maclean-Bristol, director at PlanB Consulting, and host Paul McCaffrey

Winner Daisy Shadow-Planner

The judges said: Shadow-Planner has proven to be an enormous asset to a great many companies and users. With this product, Daisy has shown that it recognises that it is people that make a business successful, and that software tools exist to enable them.

About: Formed in 2001, Daisy has grown into the UK's largest independent provider of IT, comms and business continuity with 600,000 customers, 2,000 partners and some 4,000 employees in over 35 locations nationwide. In addition to providing services to half of the country's high street retailers, Daisy is at the technological heart of the nation's critical infrastructure – from keeping trains running to planes flying; it supports doctors caring for patients and connects businesses of every kind to the customers they serve. Shadow-Planner brings all strands of a business together and identifies which parts are most critical. Its hugely powerful real-time dependency mapping capability identifies weaknesses immediately.

"Having won this award in 2016, we entered again this year because, having listened to our customers, our user group and industry-leading business continuity managers, we've taken great steps to improve Shadow-Planner so that it is more relevant and effective for the midmarket, whilst enhancing its enterprise capabilities even further," says Colin Jeffs, head of business continuity management at Daisy.

"This work is still ongoing and it means we are bringing the huge benefits of business continuity management planning software to a much wider and diverse audience.

"It is really gratifying to win this year, on top of our win when we last entered, and even better news for us and our customers is that we've been working with our user group to understand what further developments and functionality they would like to see, and there are already further great new features in the pipeline both short and longer term.

"We look forward to entering this category again once these have been rolled out and our customers are reaping even greater benefits. It's true that no two businesses are the same but having a business continuity management software product that's aligned to best practice and recognised as industry-leading is vital when considering your business continuity programme, no matter what your business does."

daisygroup.com

daisy.

20th ANNIVERSARY

WINNER
BUSINESS CONTINUITY AWARDS 2018
BCM PLANNING SOFTWARE OF THE YEAR

Shadow-Planner WINS BCM planning software of the year 2018

daisy.

Shadow Planner. BCM Software

Contact us today to book a full demonstration

T: 0344 863 3000
E: enquiry.dcs@daisygroup.com

Or come and meet us at BCI World 2018 and enjoy a "10 minute taster"

bci WORLD
Conference and Exhibition
6th - 7th November 2018
www.bciworld2018.com

Book as a visitor to attend the **FREE** exhibition and seminar programme

Or, use code **DAISY10** when you book for the full conference and receive 10% off

20th ANNIVERSARY
WINNER
BUSINESS CONTINUITY AWARDS 2018
BCM PLANNING SOFTWARE OF THE YEAR

CIR
WINNER
BUSINESS CONTINUITY AWARDS 2016
BUSINESS CONTINUITY MANAGEMENT PLANNING SOFTWARE OF THE YEAR

CIR
WINNER
BUSINESS CONTINUITY AWARDS 2015
MOST INNOVATIVE PRODUCT OF THE YEAR

CONTACT US

If you'd like would like a full demonstration of the Shadow-Planner product.

0344 863 3000 enquiry.dcs@daisygroup.com

bsi. ISO 22301 Business Continuity Management

bci Business Continuity Institute Founding Partner

we are daisy.
www.daisygroup.com

Global Award

Buti Qurwash, Dubai Airports, pictured with Scott Baldwin, CIR Awards judge, and awards host Paul McCaffrey

Winner Dubai Airports

The judges said: Dubai Airports was able to successfully demonstrate its key focus of providing corporate support and direction for delivering resilience and assurance. In so doing, it has created a 'new normal' in business resilience providing greater flexibility, creativity, global awareness, and social awareness – for which they are to be congratulated.

About: Dubai Airports (DA) owns and manages the operation and development of Dubai International (DXB) and Dubai World Central (DWC) airports. Air transport is fundamental to Dubai's social and economic development and welfare; it comprises 28% of GDP. DA is vital in creating a lasting, positive impression for tourists and residents alike. Customer experience is amongst DA's key focuses.

The Dubai Airports Corporate Resilience unit's main focus is providing corporate support and direction for delivering a resilient business model and correct levels of assurance to underpin the corporate strategy of ensuring Dubai Airports operate effectively despite major internal and external challenges. The Corporate Resilience team has delivered a programme that encompass enterprise risk management, response and recovery processes and insurance management, resulting in adequate business protection against current and future threats to people, services, operations, facility and reputation. The unit also adds value through continuous improvement recommendations and conducts reviews to produce cost effective insurance liability.

Executive vice-president, Corporate Affairs, Majed Al Joker, commented, "I am tasked with overseeing the airports' security, legal, internal assurance, excellence and resilience initiatives. It brings great pride and honor that the success of our efforts and ideas are now recognised globally. This is not a one-person feat; and I would like to thank all employees who have worked day-in and day-out to transform our company; I am pleased that Dubai Airports now belong to the élite cadre of awarded organisations for adopting leading resilience practices. I must also thank all our internal and external stakeholders and acknowledge their vital role and support in enhancing our resilience capabilities.

"We are more energised and motivated than ever to take on new and challenging projects to further improve our risk management, response and recovery capacities – both for the benefit our organisation, as well as aviation in Dubai generally."

dubai.ae

Dubai Airports
Connecting the World

20th ANNIVERSARY
WINNER
BUSINESS CONTINUITY AWARDS 2018
GLOBAL AWARD


dubaiairports.ae
WOW-Fi
DISCOVER THE WOW IN OUR Wi-Fi.
Just one click to get unlimited, free access to DXB's jaw-dropping, high-speed Wi-Fi.
#mustbeDXB
Dubai Airports
Connecting the World

Ambassador Award

Industry ambassadors, Sungard Availability Services, pictured with Jason Crosby, global business continuity manager, MUFG Securities International plc and awards judge; and host Paul McCaffrey

Winner Sungard Availability Services

The judges said: It is 20 years since the Business Continuity Awards were launched. To mark this special occasion, the board and the judging panel are presenting the Business Continuity Ambassador Gong. This award goes to the company that we believe has done the most for the industry over the life of the awards. We have no hesitation in presenting Sungard Availability Services with this accolade.

About: Sungard Availability Services is a leading provider of critical production and recovery services to global enterprise companies. Sungard AS partners with customers worldwide, truly getting to understand their business needs and provide tailored services for defined outcomes. A name that is synonymous with business continuity, Sungard AS leverages over 35 years' experience of designing, building and running critical IT services that help customers manage complex IT, adapt quickly and build resiliency and availability.

"As a pioneer in the field of disaster recovery and business continuity, Sungard Availability Services is delighted to add the inaugural Ambassador Award to our unparalleled track record of success in the CIR Business Continuity Awards," says Kathy Schneider, chief marketing officer for Sungard Availability Services. "Having advocated the benefits of availability and resilience for four decades, this accolade is fitting recognition in the year in which we celebrate our 40th anniversary.

"We extend our congratulations to all the finalists and winners, especially former customer and Sungard AS Customer Advisory Board member Steve Mellish, Hon, FBCI on being honoured with the Lifetime Achievement Award. We were also pleased to see our customer Barclays recognised for Excellence in Business Continuity in the Financial Sector.

"The Business Continuity Awards are a highly respected and much coveted industry standard for businesses continuity professionals. We're extremely proud to be recognised, along with our customers. The Ambassador Award recognises our continued commitment to deliver the highest standards of service for our customers.

"Today, more than ever, it is essential for businesses to remain resilient in the face of huge challenges. We constantly strive to deliver the services and consultancy to facilitate this mindset and work closely with our customers to help them achieve it."

sungardas.co.uk

SUNGARD
AVAILABILITY
SERVICES®

20th ANNIVERSARY
WINNER
BUSINESS CONTINUITY AWARDS 2018
AMBASSADOR AWARD

Industry views

As reported in this magazine, Airmic recently published the main findings of an in-depth report by Cass Business School into the implications of the fourth industrial revolution for business models and risk management. 'Roads to Revolution' found that existing principles of resilience need to be extended for opportunities to be realised and resulting risks managed.

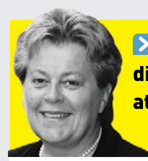
One important aspect is that of governance. In most large organisations, cyber governance has failed to reflect technology-driven changes in the way that companies are run.

Airmic recently hosted a discussion on the topic, bringing together some 20 experts from the worlds of risk management, digital risk, information security, governance, business, insurance, law and HR. All agreed that the consequences for boards of the pace of change in the networked world on which business models are now based means we must continuously revisit our cyber risk governance procedures, especially in the face of increasing regulatory and shareholder focus.

The lack of a common language was considered the main barrier to good cyber risk governance. It holds the board back in building knowledge and oversight of the risks and opportunities and in sharing its vision and risk appetite.

Cyber risk is an enterprise-wide, business-driven subject. It belongs within an ERM framework, with a line of communication to the board – probably through a risk committee or audit committee. Although technology information and security expertise are an essential part of the mix, cyber governance goes well beyond the IT department.

Before we can develop robust cyber governance, we also need to address a lack of education about the risks and opportunities of the digital world. We have to become digitally fit and comfortable with the subject. Just as people need financial literacy, the new literacy for the future is digital. There is a critical role for the risk manager here in developing a common language for cyber risks and insurance, facilitating communication and increasing awareness – maximising the chances of conveying their message by placing the discussion in a business model and value-creation context.



Julia Graham is technical director and deputy CEO at Airmic

It was the topic of much discussion... and it's finally here. Since 25th May, the EU's General Data Protection Regulation (GDPR) now applies directly to the UK and will be incorporated into UK law by the Data Protection Bill.

There have been a number of reported cases involving data breaches within local authorities due to employee actions. All of these led to fines for the offending authorities, but also had significant reputational impact.

Many of the headlines around the new rules have focused on these penalties, but the Information Commissioner's Office has been working hard to convey that, whilst the fines for breaches will be significant, the key aim is to change culture and behaviour around data control and management.

The biggest change will be in accountability. Understanding how we store and share data, what our audit trails are and how we deal with inaccurate information will be the main focus. When we get it wrong we will now be required to report a personal data breach that affects people's rights and freedoms not later than 72 hours after having become aware of it. This will be no small task. When reporting breaches it will need to include the potential scope and cause of the breach.

All public authorities must designate a Data Protection Officer but it is vital that everyone is involved in data management. Awareness of information security incident management policies, procedures and guidance, lessons learned through briefings on incidents at their own or other organisations, reminders through emails, intranet, newsletters and team meetings are all good examples of disseminating messages. And these need to be done regularly.

Alarm is committed to helping members work their way through the considerable task of GDPR compliance – including some reflection on the opportunities as well as the risks. As an example, better control of data can simplify and in some cases automate processes. This in turn could lead to better ways of using the data for service delivery and more effective engagement with the public.

Mandy Knowlton-Rayner is a board director at Alarm

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

At a recent conference on insurance regulation, the mood about the new world of Solvency II was decidedly downbeat. The feeling was that too many cooks were spoiling the broth. From the more prescriptive elements of the EU legislation to the layers of justification needed for any approach that deviates from convention, regulation was portrayed as a significant brake on innovation and the exercise of common sense.

It felt as though the ideals of Solvency II – of regulating insurance companies according to the unique mixture of risks taken by each one – has given way to a multi-stage approach to decision-making and supervision, where each stage adds a little caution and distils out a little innovation.

Part of me wondered what all the fuss was about – after all, the introduction of the then Financial Services Authority's risk-based regime in the early 2000s, demanding accurate pricing of guarantees, created havoc in the insurance sector – forcing recapitalisation and demutualisation in its wake. As it bedded down, the FSA regime became more popular and trusted by insurers, and now it is even looked back upon with a certain amount of nostalgia. However, some of the concern is well-founded; if Solvency II ends up as an exercise in providing the illusion of risk management, when all that is really happening is the performance of a ritual designed to protect those making decisions from future criticism, we will end up trivialising the practice of risk itself. Part of the problem is the idea that risk management is about stopping bad things from happening, so stopping most things from happening is a good second best.

In the late 20th century, environmentalists started to talk about sustainable growth, rather than stressing the incompatibility of economic growth with protecting the environment. In doing so they gained many allies and made tangible progress in achieving their aims. In order to overcome the challenges set by Solvency II, the risk management profession needs to find a similar formula that captures the tension between risk and innovation; perhaps a concept of 'sustainable innovation' may go some way to achieving this.

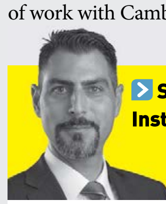
Dr Matthew Connell is director of policy and public relations at the Chartered Insurance Institute

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

As we hit the balmy summer, the Institute is by no means slowing down. We've launched our new joint training course for infrastructure risk with Turner and Townsend and are readying ourselves for the official launch of the new Certificate in Digital Risk Management. We have also published our first Asia-Pacific newsletter with the help of our growing Global Ambassador network, which now spans the Asia-Pacific and Oceania regions, India, the countries of South East Asia, China, Japan, Australia and New Zealand.

At the same time, my tenure as chairman for the Institute of Risk Management is well underway, and I'm keen to further engage with the risk community. My earliest interaction with the profession was in the mid-90s working as a student civil engineer on the London Underground Jubilee Line extension. Twenty years ago, risk management was primarily health and safety driven. I was preparing method statements, permits to work, and performing site risk assessments. Moving through university, I was one of the first post-graduate students from Cass Business School's Master of Science in Insurance and Risk Management. I followed the natural route – as many others did at the time – into the insurance industry. It was in the early 2000s when I first got a taste for risk management with a truly international and multi-sector focus. I was building risk registers, working with risk owners and preparing key risk indicators and risk reports. By the mid-2000s, ERM frameworks were introduced bringing together fragmented risk management efforts.

I am keen that the Institute continues to champion enterprise risk management as a profession and to ensure industry talents is both current and competent. Therefore I am pleased to say that we are building on our Risk Agenda 2025 project to help plug skills gaps and enable our members to keep abreast of changing regulations and the most current thinking in the field. To bolster this effort, we've some exciting thought leadership projects nearing fruition, including a major body of work with Cambridge Judge Business School.



Socrates Coudounaris is chair of the Institute of Risk Management

In association with irm

Crisis of confidence?

Companies are overestimating themselves when it comes to crisis preparedness, representing a new and potentially dangerous risk dynamic against a backdrop of growing crises, according to a study from Deloitte

Organisations are keenly aware of the increasing threat of crises, yet many may overestimate their capabilities to respond. This is among the conclusions of Deloitte's latest crisis management survey, which found that 60% of organisations face more crises today than they did ten years ago.

The study, which surveyed over 500 senior crisis management, business continuity, and risk executives about crisis management and preparedness, uncovered considerable gaps between a company's confidence that they can respond to crises and its level of preparedness. The gap becomes even more evident when evaluating whether organisations have conducted simulation exercises to test their preparedness.

"With the rapid pace of change facing companies worldwide, and with crises on the rise, it is critical for organisations to be ready to respond with skilled leadership and plans that have been tested and rehearsed," says Peter Dent, global crisis management leader at Deloitte. "Organisations that are adept at crisis management take a systematic approach to steering clear of potential crises and managing those that do arise with an eye to both preserving and building value."

Nearly 90% of respondents say they are confident in their

organisation's ability to deal with a corporate scandal, yet only 17% of organisations have actually tested the assumption through simulation. The gap is reminiscent of Deloitte's 2015 findings, which illuminated the fact that board members believed they could respond well if a crisis struck, yet playbooks of likely scenarios failed to exist.

The study found that 80% of organisations have had to mobilise their crisis management teams at least once in the past two years. Cyber and safety incidents in particular have topped companies' crises (46% and 45%, respectively).

Following a crisis, nearly 90% of organisations have conducted reviews, according to the study. The major insight from these examinations is that many crises may have been averted. This appears to prompt organisations to take action to forestall future crises. Respondents identified the need to improve detection and early warning systems, invest more effort in prevention, and do more to identify potential crisis scenarios.

"Crisis management shouldn't start with a crisis – at this point it may already be too late. The ability to prevent a crisis can be fortified by looking at the entire life cycle of a crisis instead of just readiness and response," continues Dent. "Successful crisis management also requires overcoming any biases to ensure that the board and senior management look closely at risks. Even those, and perhaps especially those, they believe aren't likely to happen."

Written by Deborah Ritchie

Responding to a crisis

Strong leadership skills and situational awareness are critical. The survey finds that nearly a quarter (24%) of respondents cite the effectiveness of leadership and decision making as one of their greatest crisis management challenges.

To help leaders be prepared to navigate their organisations through a crisis, organisations should consider: organising leaders ahead of time, clearly defining their various roles and responsibilities; training leaders in the tools and techniques that can help them through a crisis; identifying, improving and counterbalancing leadership tendencies and styles which, while they may serve as strengths in normal situations, could cause trouble in a crisis.

Board and senior management participation in crisis exercises is critical, as is their involvement in developing an organisation's crisis plan. More than four in five (84%) respondents say their organisations have a crisis management plan in place, and those who enlist the board to participate say the number of crises has declined over the last decade (21%), compared with those without board involvement (2%).

Source: Deloitte

BUSINESS CONTINUITY SOFTWARE

clearview
Making the Complicated Simple
CIR BUSINESS CONTINUITY AWARDS
WINNER 2012/2013/2014/2015/2017
BUSINESS CONTINUITY MANAGEMENT PLANNING SOFTWARE OF THE YEAR

ClearView Continuity
Astral House
Granville Way
Bicester
Oxfordshire
OX26 4JT

Tel: +44 (0)1869 354230
www.clearview-continuity.com

ClearView BCM Software
Developed through a combination of practical experience of BCM consultants, live client feedback and technology experts, ClearView has quickly become a leader in the global BCM software market.

ClearView has removed many of the barriers that organisations experience when implementing BCM software, ensuring that ClearView delivers improvement to their BCM processes.

- Delivers ease of use for straight-forward, effective deployment and maintenance of BIA's, plans, exercises, risk and incident management. Users do not need extensive training and can pick up and use ClearView quickly and easily, even if only accessed infrequently
- Achieves a high level of modularity which means that configuration allows the solution to meet the needs of organisations precisely, but in a very cost effective manner
- Accessible from any web browser and mobile device, with mobile applications for all major platforms.
- Provides alignment to ISO22031 and Regional BCM standards
- Fully integrated Emergency Notifications and dynamic Incident Management module
- Winners of BCM Software of the Year for an unprecedented 5 years between 2012 and 2017.
- Fully ISO 27001 (information security management) and ISO 9001 accredited to provide the highest levels of security and robustness. Trusted by international private and public sector organisations
- Implemented by consultants with many years BC experience so we understand exactly what you want and can offer professional help. Much more than a software service
- Backed up with global support for clients in all sectors and all sizes
- Comprehensive reporting and dashboard analysis plus a custom report builder and integrated What If?/GIS capability for scenario mapping

ClearView – we make the complicated simple.

Shadow Planner
BCM Software

Contact Daisy to find out more about the unique benefits of Shadow-Planner:
Call +44 (0)344 863 3000
Email enquiry.dcs@daisygroup.com
https://daisygroup.com/campaign-shadow-planner

daisy.

Daisy Shadow-Planner enables you to plan, develop, test and execute more streamlined and structured Business Continuity. Taking the pain out of the entire process, Shadow-Planner helps your people work smarter and faster and enables your business to deliver against its BC commitments more quickly, efficiently and cost effectively.

Designed by BC specialists, this suite of integrated software supports the entire Business Continuity Management (BCM) lifecycle: from impact analysis through developing plans to testing and reporting. Daisy supports you every step of the way, helping you create the strongest and most effective plans to minimise downtime and ensure you can work 'business as usual'.

Shadow-Planner is based on four core modules:
- Business Impact Analysis (BIA)
- Business Continuity Planning
- Notification
- Mobile Plans

Organisations in the financial services sector, public sector and others in regulated industries have used Shadow-Planner to help comply with business continuity standards such as ISO 22301 and other specific codes of practice.

How you benefit
A low-cost solution, requiring no local cap ex or hardware investments, you can:
- Get rid of inefficient, inaccurate and risky manual approaches - Word documents and spreadsheets
- Ensure all essential data (plans, contacts, documentation and more) are in a single secure location, at your fingertips
- Be assured that all data is regularly reviewed, updated and consistent
- Achieve faster ISO 22301 BC certification

BUSINESS CONTINUITY SOFTWARE

ParaSolution is a web solution simplifying and managing Business Continuity, Disaster Recovery, Risk Management and Emergency Management over the last 15 years. ParaSolution is proven in large and small organizations including the financial sector, manufacturing and governmental agencies. With always the client at the heart of our considerations, here are key features:

- EASY TO USE, thanks to its re-engineered user interface and automated workflows sending reminders.
- EFFICIENT, since information captured in the BIA is automatically available in other steps of the lifecycle and connected to a centralized and integrated database including stakeholders contact information.
- MULTILINGUAL, the solution communicates with users in their preferred language (interface and notifications).
- ParaSolution comes with standardized templates, based on industry best practices such as ISO 22301 and BCI Good Practices, while allowing EXTENSIVE CUSTOMIZATION to suit your organization's needs.
- MEASURE compliance to ISO 22301 using integrated ICOR self-assessment tool and obtain guidance in progression.
- ParaSolution SaaS is highly available, hosted on secured and audited servers and can also be hosted by your organization.

Premier Continuum Inc., proud developer of ParaSolution, is a training partner of the BCI and of ICOR and a consulting firm with hands-on experience, celebrating its 20th anniversary.

Premier Continuum
1010, Sherbrooke West, #800, Montreal (Quebec), H3A 2R7, Canada

Tel: +1.514.761.6222
Toll-Free: +1.877.761.6222
info@premiercontinuum.com
www.premiercontinuum.com
Twitter: @1continuum

Sungard AS Business Continuity Management Planning Software

Assurance^{CM}

Brand new to this edition of the report is **Assurance^{CM}** which was designed by users, for users. This next-generation business continuity software and risk management solution removes the barriers to organisation-wide engagement and builds greater confidence in contingency plans. It's about extending beyond simply addressing compliance requirements. It's also about knowing teams are prepared to recognise threats to the business and empowering them to engage locally before incidents lead to major disruptions.

So far our users rate the **Assurance^{CM}** experience as:

Intuitive – Simple and easy, get your program up and running with minimal training
Aware – Merge external happenings with enterprise plans and gain real-time contextual insight to act decisively
Alive – Eliminate manual data management and trust that your data is accurate and up-to-date
Efficient – Yet secure to help you work smart, engage users and delight stakeholders on program effectiveness
Independent – SaaS and mobile, connect quickly to people and information that matters the most

And a 100% SLA availability guarantee.

Plans and testing do not deliver outcomes, people do. **Sungard AS Assurance^{CM}** is about enabling you to take what we learn back into the business continuity/disaster recovery planning cycle and share it across the company for better outcomes.

ASSURANCE^{NM} (NOTIFICATION MANAGER)

Introducing our new powerful emergency notification tool, designed for when you need it most to ensure the effect send of critical alerts to your key recipients at any time, using any device, and get the response you need.

Assurance^{NM} Alerting and Mobile Services from Sungard Availability Services (powered by Send Word Now®) leverages a variety of communication methods to transmit tens of thousands of voice and text messages in minutes. The Assurance^{NM} communication solution is built on an award winning platform that is used by both public and private sector organisations worldwide, offering them market leading capabilities and superior performance which Sungard AS customers can rely on. For more information please contact Sungard AS:

UK & European Head Office
Unit B Heathrow Corporate Park,
Green Lane, Hounslow,
Middlesex
TW4 6ER

Tel: + 44 (0) 800 143 413
infoavail@sungardas.com
www.sungardas.co.uk

US & RoW
680 East Swedesford Road
Wayne, PA 19087 USA

Toll-Free: 1 800-478-7645
Local (US): 1 610-878-2644
Email: AS.SoftwareSupport@sungard.com
www.sungardas.com

BUSINESS CONTINUITY, DISASTER RECOVERY & ALWAYS ON INFRASTRUCTURE

daisy.

For more information:
Call +44 (0) 344 863 3000
Enquiry.dcs@daisygroup.com
www.businesscontinuitytransport.com

Daisy has become the UK's go to partner for resilient, secure and always available communications and IT infrastructure managed services.

As the UK's business continuity industry leader with over 25 years' experience, Daisy is embedding resilience into its entire service portfolio, focussed on enabling today's digital business in the key areas of always-on infrastructure, connect & protect and agile workforce.

Business Continuity Management:
Daisy's BCM consultants and Shadow-Planner software work with you to deliver digital business resilience and address the new risks of the digital economy. We advise, deliver, support and manage all or part of your business continuity management, including emergency response planning; crisis and reputational risk management; operational and business recovery planning; infrastructure process and IT risk analysis; supply chain risk management; authentic exercising, maintenance and awareness.

Workplace and FlexPlace Recovery:
Daisy has got your offices and your people covered from 18 specialist business continuity centres available UK-wide, mobile and virtual office solutions delivered to the home and complex call centre and financial trading positions. We usually have customers up and running within an hour and not just for business interruptions, but to cope with peak or seasonal trading and the flexibility digital businesses now demand.

ITDR, FlexTech and Data Availability:
Daisy's flexible IT and data recovery services will protect your technology, data and communications, available when the need arises and for test and development scenarios. We have nine resilient UK data centres and an award-winning portfolio of data availability services, applauded by industry analysts. For replacement IT onsite fast, we have over 1,000 servers and seven ship-to-site, mobile data centre units, all ready to dispatch if disaster strikes. This can be a safe roll-back recovery option in the event of cyberattack.

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.

CLAIMS HANDLING & RISK MANAGEMENT SOFTWARE SOLUTIONS

JCAD

JC Applications Development Ltd
Manor Barn, Hawkley Rd, Liss,
Hampshire, GU33 6JS

Contact: Phil Walden

Tel: +44 (0)1730 172020
sales@jcad.co.uk
www.jcad.co.uk
Twitter: @jcad2

In business since 1992, JC Applications Development Ltd take great pride in our ability to develop world class software solutions and associated services that enable our clients to manage risk, compliance and claims more effectively. As a result they are better placed to achieve their corporate ambitions, save time, money and offer a superior service to their stakeholders. This is proven by our last customer satisfaction survey where 98% of respondents said that they would recommend us.

With over 200 successful implementations JCAD is a market leader in the provision of claims handling and risk management software to both the public and private sectors. Client representation covers many diverse industries including but not limited to;

- Housing associations
- Local government
- Emergency services
- Charities & NGO's
- Academia
- Finance
- Retail
- Construction
- Facilities Management
- Utilities

JCAD's software is wholly "off the shelf " which enables time efficient implementations, low cost systems and simpler training. Additionally, by offering a best practice approach to risk and compliance management we can focus on the development of new functionality that is then shared across our entire client base. JCAD are an ISO9001 accredited supplier and our hosting partners are accredited to ISO27001.

CLAIMS HANDLING & RISK MANAGEMENT SOFTWARE SOLUTIONS

ventiv TECHNOLOGY

Ventiv Technology
30 – 40 Eastcheap, London, EC3M 1HD

Contact: John Irving

Tel: +44 (0) 20 3817 7407
john.irving@ventivtech.com
www.ventivtech.com
Linkedin: www.ventivtech.com/linkedin
Twitter: @ventivtech

RiskConsole Advance
Whether you're managing risk, safety or insurance programs, your job is more challenging than ever. More data. Increased business complexity. Greater security risks. Heightened expectations. Less time to respond, and with fewer resources.

RiskConsole Advance empowers you to take control of your organisation's data and achieve the clarity you need to make fully informed decisions. Improve your efficiency and maximize scarce resources—while getting back the time you need to think and act strategically.

Fully embedded and integrated into RiskConsole Advance, Ventiv's analytics, reporting, and data-discovery platform is the market's newest, most technologically current offering. Ventiv is the only RMIS provider offering cutting-edge **IBM Watson Analytics** as an embedded, integrated component of our solution. When you add it up, RiskConsole Advance's comprehensive analytics, reporting, and data-discovery empowers you to make data-driven decisions that generate optimal outcomes like reducing claim frequency and severity.

With your processes optimized, best practices embedded and knowledge converted, you have raised your risk technology maturity level to drive better results and make your risk management department more resilient.

WORK AREA RECOVERY

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

Fortress is London's first independent work area recovery centre provider in over a decade.

We provide modern, flexible and more relevant work area recovery services to London and around the world.

Our modern facilities provide a bright and current environment designed for agile and collaborative working. The aim is to provide a replica of a modern office, somewhere comfortable and familiar where your staff feel happy to carry on business as usual.

We always support your recovery, in test and in invocation, in person and onsite with our highly experienced recovery technicians. We also give you control over your recovery environment and that gives you faster recovery.

Fortress values our customers and we will always deliver local, high touch, service led interactions from both a commercial and technical perspective.

So please get in touch and we will be pleased to explain how we are different and how we can help you provide your organisation a more modern and relevant solution to their work area recovery needs.

You're Prepared
London Prepared

Promoting business continuity in the City of London

London is one of the world's great cities – a global centre for business and commerce. Ensuring London is ready to meet the challenges of tomorrow is fundamental to the world economy and a priority for the City of London and every London business.

DOMINE DIRIGE NOS
CITY OF LONDON

LONDON PREPARED
Resilience Through Planning

www.cityoflondon.gov.uk/businesscontinuity


Robotics, drones, prefabrication
Construction sites are changing. 500,000+ industry roles could also transform within 20 years.
Prepare your business with a combined construction policy from QBE.
_ Tailored to your requirements
_ Empowered experts
_ Sector experience as standard
_ Chosen by 22 of the UK's top 25 contractors
QBE. Our business is knowing yours.
QBE