The interview
Andrew Slevin discusses accurate declared values

Book review
Crisis Proof: How to prepare for the worst day of your business life

Executive summary
FM Global addresses global quake risk

cirmagazine.com

May-June 2021

CIR
CONTINUITY INSURANCE & RISK

Building back better? *Upbeat projections for the UK construction sector mask some serious reputation and risk issues*

The tempest threatens *Today's directors and officers face a vast and ever-expanding array of potentially costly liabilities*

Feeling the heat *The consequences of climate change, including the transition itself, are changing risk and operating environments*

Cyber insecurity

Resilience for the new normal

View: "The disruption from the Suez closure could cause companies to move away from just-in-time supply chains towards keeping much higher inventory levels – a tectonic shift that will impact insurers hugely"

Comment

Readers of this magazine don't need to be told that cyber security breaches pose a serious threat, but the extent of the situation according to the government's latest report on the state of cyber security among UK businesses warrants mention.

The 2021 *Cyber Security Breaches Survey* describes the degree to which cyber risk has heightened amid the pandemic, as organisational resources have been diverted to facilitating home working, and the usual security measures have in some cases been almost completely bypassed.

According to the data, the most common breaches or attacks were phishing emails, followed by viruses or other malware, including ransomware.

The study shows that fewer businesses are using security monitoring tools to identify abnormal activity that could indicate a breach, which suggests firms are less aware than before of breaches and attacks. The number of businesses with up-to-date anti-virus software is also down from the previous year, at 83 per cent.

The figures also reveal that nearly half of businesses have staff using personal devices for work, but only 18 per cent have a cyber security policy on how to use those personal devices for business purposes.

Despite these findings, respondent businesses report that cyber security is a high priority; 77 per cent said it was key.

It is clear that there is a disconnect between good intentions and what is actually happening on the ground – pointing to a genuine need for greater resilience in cyber security programmes.

Most strikingly, fewer than 23 per cent of the businesses polled for this major report have a cyber security policy covering home working at all. This is a problem when you look at the numbers of employers and staff heading down the hybrid road towards their new normal.

Despite the pandemic (or because of it?) the UK's cyber industry attracted record investment last year. The sector is now worth an estimated £8.9 billion, according to the government's annual *Cyber Sector Report*, which puts the number of people employed in UK cyber security at around 50,000, and the number of active cyber security firms is up 21 per cent on the previous year.

The sector contributed more than £4 billion to the economy in 2020, attracting some £800 million of investment. The most commonly provided products and services included cyber professional services, threat intelligence, monitoring, detection and analysis, with major growth areas identified in industrial control systems and IoT security – a signal, the report's authors say points to the sector's adaptation towards such emerging challenges as the need to secure smart cities. And these smart cities won't just be in the capital, as this year's report suggests that more than half of these firms are now based outside of London and the South East, with clusters of activity proliferating in Scotland, Northern Ireland and North West England, among others.

This is good news in theory for the government's 'levelling up' agenda – but remote working cannot work without appropriate – or at least adequate – cyber security.

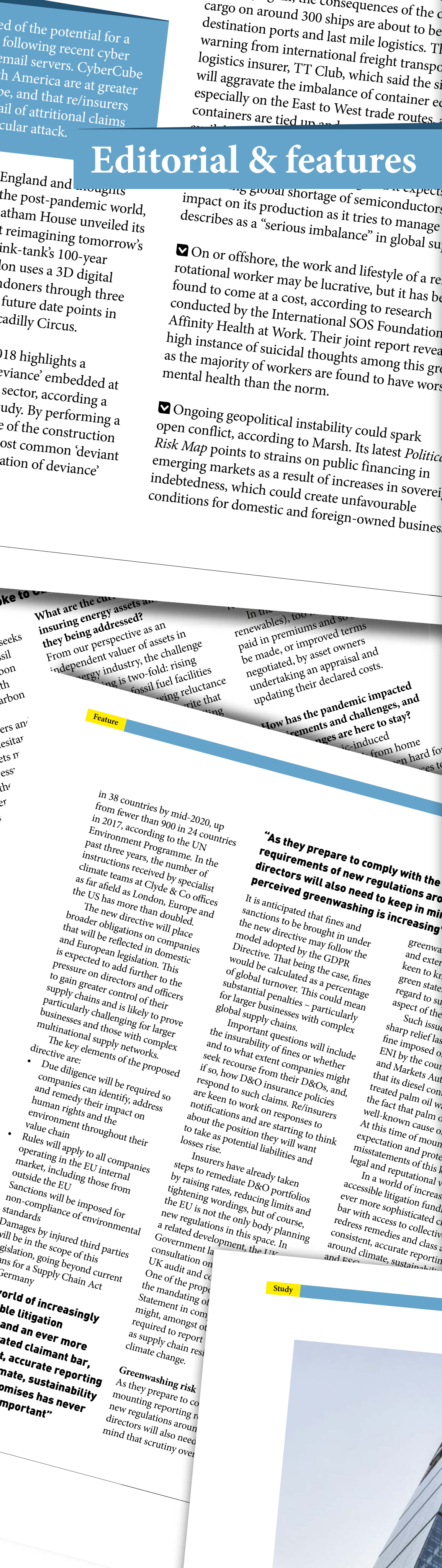
Over a year has passed since the coronavirus pandemic was declared, forcing companies to adopt new working practices to ensure business continuity. Now, as restrictions begin to ease again and businesses consider their new normal after many months with entire workforces operating from home, questions about how hybrid working strategies will work in practice need addressing. And that includes considering the role of cyber security as an enabler for this blended – and hopefully secure – new approach.

Deborah Ritchie

COVER STORY

Cyber insecurity

Editorial & features



News, views & regulars

CIR

CONTINUITY INSURANCE & RISK

Group 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

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

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, EC2M 5PD
UK

Tel: +44 (0)20 7562 2400

ISSN 1479-862X
cirmagazine.com

Flexible Serviced Workplace Solutions from Sungard Availability Services

Organisations in the post-pandemic world need office space that is flexible, resilient and secure. That's why Sungard AS introduced *Serviced Workplace*, a service that delivers the flexibility organisations today require.
No invocation needed.

- **100% available office space in dedicated suites, tailored to your precise requirements**
- **Ability to 'drop in,' with badge, to other Sungard AS facilities across the UK and Ireland**
- **Fully-hardened, facilities following best-in-class security procedures**
- **The option to recover to another Sungard AS facility**

Serviced Workplace Solutions from Sungard AS enable you to navigate the business challenges of the post-pandemic world while giving your workforce the ability to work, rest and recover from any disruption — anytime, anywhere.

To learn more about *Serviced Workplace* from Sungard AS please visit www.sungardas.com or call us on 0808 238 8080.

Digital first

The pandemic has turbo-charged the shift to virtual care. In this fast-paced environment, insurers will need to evolve if they are to support digital health providers in reaching their full potential. Jennifer Schoenthal writes

The global digital health and wellness sector is at a point of inflection. The public is receptive. Health systems are keener than ever to harness the cost and efficiency gains it promises; market players are keen to make the most of the opportunities. But fresh capital, new technology and above all, robust risk management, are essential if the sector is to meet its potential.

According to Beazley's own research, 89% of market participants feel they are operating in a moderate to high-risk environment. They are concerned about both insurable and uninsurable risks, those that affect the sector as a whole and risks that are particular to their types of business.

Given these high levels of concern, it is alarming that 70% of businesses have cover for only one or two key risks. Indeed, across the board, over two thirds of businesses lack cover for existential risks including loss of personal (medical) data; system failure or cyber hack resulting in bodily injury; and medical malpractice due to the provision of remote care.

Over 60% of businesses also lack cover for medical malpractice due to incorrect data; technology error resulting in bodily injury or financial loss; and system failure or cyber hack resulting in financial damage.

One of the reasons why insurance penetration is so poor, even though industry leaders are confident they understand the insurance cover they need, is the sheer complexity of the risks.

Healthcare and lifestyle professionals are well-versed in medical malpractice, bodily injury and professional liability exposures, but many are unaware of the risks that arise when they move their business online, such as data privacy and protection, cyber risk, technology product liability and media liability risks.

Likewise, technology businesses typically understand cyber and data breach liabilities and product liability, but may not be aware of the bodily injury, medical malpractice, or the professional liability risks they may face if the technology fails or malfunctions or if a cyber breach occurs.

In the past year, digital health providers have expanded their online presence to provide more advice. The speed of the switch to this new mode of care has left little time to implement relevant training around the associated professional indemnity risks.

Similarly, disease testing and diagnosis via track and trace or similar systems has been rolled out globally at speed and scale, but the wealth of personal medical information has attracted the attention of hackers, putting unexpectedly high levels of stress on service providers' data privacy policies and technology product liability policies.

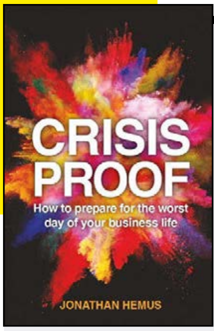
In this fledgling industry, the pattern of insurance claims in the digital health space is still emerging. For the moment, many courts remain closed or are operating on a reduced basis and a deep stock of goodwill towards the medical profession in light of its response to COVID-19 is likely delaying potential claims.

Looking ahead, the insurance 'ask' will become even harder. The creation of new digital health products and services, the adoption of new models including more remote working, and investment in technology and artificial intelligence are all strategies identified by digital health businesses to sustain growth in 2021. Such developments, while essential to the future of the digital health industry, will add further pressure on the insurance industry to adapt and evolve new covers.

As an industry we will need to educate the market about the unique range of complex, interconnected risks it faces, not just around diagnosis, treatment and care, but also technology, data privacy and compliance. Solutions will need to be integrated, to reduce the potential for gaps and duplication and to offer seamless cover combining medical malpractice, product liability, cyber and technology E&O with bodily injury protection.

Jennifer Schoenthal is global product leader, Virtual Care at Beazley

Inspiration for resilience professionals



Crisis Proof: How to prepare for the worst day of your business life

Jonathan Hemus, Rethink Press, 2020. Reviewed by Deborah Ritchie, editor, CIR

rethinkpress.com

We're all looking for a good night's sleep, and here's a book that promises to provide that by making sure you're always prepared for "the worst day of your business life" – always ready to protect your business and reputation, whatever the world may throw at it.

This book, published just before the end of one of the most tumultuous years in recent history, is an extremely accessible guide to crisis management for professionals that are completely new to the practice.

Presented in a thoughtfully sequenced series of chapters, covering foundational considerations, beginning a crisis management programme and building resilience through scenario planning, *Crisis Proof* offers a 'crisis 101' for beginners – complete with quotes and tips from industry practitioners, many of whom are well known names in the field, and indeed a good number are respected CIR Business Continuity Award winners.

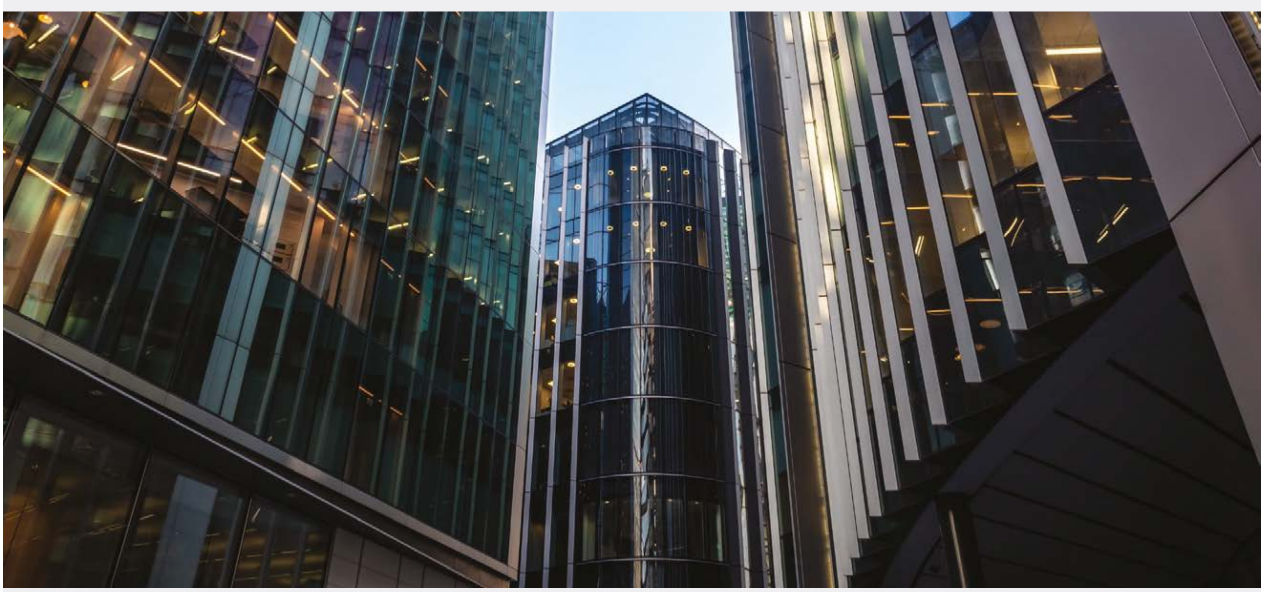
"Crises don't destroy businesses. It is the organisation's response to the crisis that does that"

Crisis Proof promises to instil confidence and clarity around the requirements that will help your business deal with a crisis, to teach you how to create and embed a crisis-resistant culture, to convey the real purpose of crisis management plans and critical content, and to help you create a high performing crisis management team. Ultimately, it aims to communicate the essential characteristics of successful crisis response – whatever the situation.

"It's all here – from Gerald Ratner's now infamous gaffe at that fateful 1991 Institute of Director's Annual Conference, to the 2015 football scandal and billionaire Richard Branson's dubious decision-making during the coronavirus crisis"

Author Jonathan Hemus – a crisis management consultant with some 25 years' experience – uses a range of example crises through which to convey his learning – from Gerald Ratner's now infamous gaffe at that fateful 1991 Institute of Director's Annual Conference, via the 2015 football scandal to billionaire Richard Branson's dubious decision-making during the coronavirus crisis.

"Crises don't destroy businesses. It is the organisation's response to the crisis which does that," Hemus writes. Mishandled crises can devastate businesses, lives and livelihoods. If you're looking to succeed in a new role as your organisation's crisis management champion (or you're hiring into the role or training a new recruit), this might just be the book for you.



News briefing

A round-up of the latest industry news

Operational resilience was found to be the top priority for financial services firms, as the sector reported the most significant improvement in optimism since December 2013. So said the latest CBI / PwC survey of the sector covering Q1. Respondents also reported continued growth in profitability, with all sectors except banking experiencing profits growth.

A separate study found that businesses in general were more concerned about competition, technology-impacted processes and regulation than they are about COVID-19, signalling a shift in focus beyond the pandemic. The study, conducted by global consulting firm, AlixPartners, suggests that executives have already begun to plan for new waves of disruption in a post-pandemic world.

Insurers were warned of the potential for a large volume of claims following recent cyber attacks on Microsoft's email servers. CyberCube said companies in North America are at greater risk than those in Europe, and that re/insurers are likely to see a long-tail of attritional claims resulting from this particular attack.

As the lockdown eased in England and thoughts turned to the new normal in the post-pandemic world, London-based think-tank Chatham House unveiled its future-gazing project aimed at reimagining tomorrow's cities. Released to mark the think-tank's 100-year anniversary, Futurescape London uses a 3D digital model to follow a family of Londoners through three generations, and imagines four future date points in the life of London's beloved Piccadilly Circus.

The collapse of Carillion in 2018 highlights a pervasive culture of 'corporate deviance' embedded at the heart of the UK construction sector, according a London South Bank University study. By performing a qualitative analysis on the collapse of the construction giant, researchers identified the most common 'deviant practices' and sources of 'normalisation of deviance' embedded in the sector.

…the government launched a consultation on a series of wide-ranging proposals for reform of the UK's audit and corporate governance regime in the wake of large-scale company failures such as Carillion, Thomas Cook and BHS.

While traffic in the Suez Canal is now moving normally again, the consequences of the delays to cargo on around 300 ships are about to be felt by destination ports and last mile logistics. This was the warning from international freight transport and logistics insurer, TT Club, which said the situation will aggravate the imbalance of container equipment especially on the East to West trade routes, as laden containers are tied up and consequently empty availability to reposition to shipment areas worsens.

…electronics giant Samsung said it expects the continuing global shortage of semiconductors to impact on its production as it tries to manage what it describes as a "serious imbalance" in global supply.

On or offshore, the work and lifestyle of a remote rotational worker may be lucrative, but it has been found to come at a cost, according to research conducted by the International SOS Foundation and Affinity Health at Work. Their joint report revealed a high instance of suicidal thoughts among this group, as the majority of workers are found to have worse mental health than the norm.

Ongoing geopolitical instability could spark open conflict, according to Marsh. Its latest *Political Risk Map* points to strains on public financing in emerging markets as a result of increases in sovereign indebtedness, which could create unfavourable conditions for domestic and foreign-owned businesses.

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

Following a spate of anti-lockdown protests, Black Lives Matter demonstrations and attacks on police forces, damages and disturbances from riots, protests and other forms of civil unrest are now among the main political risk exposures for companies in the UK and worldwide. Political violence can cause business disruption beyond physical property damage, and the ongoing pandemic and related restrictions have further fuelled disturbances. In the light of these developments, risk experts at Allianz Global Corporate & Specialty warned retail companies in particular to ensure that business continuity plans are fit for purpose.

…good news then that the pandemic was found to have accelerated the introduction of more structured business continuity programmes, with a greater expectation of investment in the year ahead, according to the Business Continuity Institute's 2021 *Horizon Scan Report*.

The FCA launched a campaign to encourage individuals to report wrongdoing in financial services. The campaign, 'In confidence, with confidence' includes materials for firms to share with employees, and stresses the confidentiality processes in place to protect whistleblowers.

Supply chain risk management organisation, CHAS announced a partnership with the University of Nottingham Rights Lab to undertake a research project around the risk of modern slavery within construction supply chains, with a focus on SMEs. Under the Modern Slavery Act 2015, there is no legal requirement for businesses with a turnover of less than £36m to publish a statement regarding how they are addressing the risk of modern slavery. However, many construction SMEs are asked by their supply chains to evidence steps to tackle the issue.

Insurers urged the construction industry to embrace reform in order to help improve the provision of professional indemnity insurance for the sector. The International Underwriting Association called for continuing improvements to regulation and culture, prioritising quality construction and safety over cost-cutting.

Two-thirds of CEOs and other C-suite executives in the UK reported having experienced decision paralysis as a result of cognitive overload or fatigue, with roughly the same number considering decision-making to be more complicated than ever before. This comes at a time when quality decision-making is paramount.

The Swiss Re Institute said insured losses from all 2020's disaster events globally were £65bn, the fifth highest in more than 50 years. It said global insured losses from natural catastrophes were £59bn in 2020; man-made disasters resulted in £6bn insured losses. Secondary peril events accounted for more than 70% of the natural catastrophe insured losses.

Despite broad optimism about the future of the digital health sector, some business could be unnecessarily exposed to financial and reputational damage through underinsurance. This was among the findings of a new report from Beazley on emerging attitudes to risk and insurance among telehealth, mobile health, health software and life sciences technology companies.

News briefing

A round-up of the latest general insurance news

The Financial Conduct Authority detailed a more generous timetable for insurers to make changes if the regulator issues new rules following its consultation on general insurance pricing practices (CP20/19). The FCA will publish any new rules at the end of May. Initially, it had said insurers would have four months to enact changes.

Insurance brokers and intermediaries reported 15 conduct rule breaches between 9th December 2019 and 31st August 2020. This is from a universe of more than 6,000 solo-regulated insurance intermediaries with a regulatory responsibility to inform the FCA each year of any conduct breaches by certified staff. These figures come from a FoI request submitted by consultant Sicsic Advisory.

MS Amlin has extended its reach into the US managing general agent market with the acquisition of International Transportation and Marine Office, LLC and its associated subsidiaries. The primary subsidiary, International Transportation and Marine Agency, LLC, provides marine and other specialty lines of insurance and will write business into Syndicate 2001.

The Competition and Consumer Commission of Singapore sought public feedback on the proposed merger of Aon and Willis Towers Watson. The consultation period was open for just one week. The proposed merger was announced over a year ago in March 2020.

Jaguar Land Rover on-demand rental platform, The Out selected Flock's usage-based insurance for its fleet. Launched by Jaguar Land Rover's mobility venture capital arm, InMotion in 2019, the rental service allows customers to hire vehicles online and have them delivered to their homes or offices.

Lloyd's posted an aggregate market loss of £0.9bn for 2020 (2019: £2.5bn profit), including net incurred COVID-19 losses of £3.4bn after reinsurance recoveries. The market's combined ratio deteriorated to 110.3% (2019: 102.1%). Gross written premiums for the year dipped slightly to £35.5bn (2019: £35.9bn) despite average premium rate increases of 10.8%.

Working remotely increased the amount of contact UK commercial brokers have with clients, according to GlobalData's 2021 *UK Commercial Brokers Survey*. Just over half of the respondents to its survey said they were in touch with clients more often now than before the pandemic. Just under half believed their relationships with customers had strengthened. It did not give details of what the other half thought.

Aviva launched a new digital cyber product with indemnity limits ranging from £25,000 to £2m with independent limits applying to first and third party cover. The insurer also joined forces with cyber security partners CyberSmart and Kaspersky to provide risk management solutions.

Allianz agreed to buy Aviva Poland for a cash consideration of £2.14bn. The sale is part of Aviva's strategy to focus on operations in the UK, Ireland and Canada. It is the eighth transaction Aviva has announced in as many months as part of its divestment process.

RAC Insurance set up its own personal lines broker, targeting gross written premiums of £300m by 2023. Telematics motor insurance will be offered first, with van and home insurance propositions to follow. RAC Insurance has appointed CDL as its technology provider. Europa Group will provide policy administration services and a branded contact centre.

For the full story behind all these headlines, visit insurancetoday.co.uk

Research from the Chartered Insurance Institute uncovered a split in customer priorities when purchasing personal lines, created by COVID-19. Those heavily affected by the pandemic put more value on clarity and choice around claims, while those who have not been financially hit still prize low premiums.

Ardonagh Group posted a loss of £206.3m for the year ended 31st December 2020, compared with a loss of £74m reported the previous year. It said this was largely due to new borrowing issued in July 2020, increased financing costs and an increased tax charge for the year. Ardonagh announced an operating profit of £47.1m for the year (2019: £3.4m), driven by acquisitions and the delivery of cost savings.

Open-source catastrophe modelling platform, Oasis Loss Modelling Framework secured £1.5m in further investment from a group of re/insurers comprising Aon, Allianz, AXA, Chubb, Guy Carpenter, Hannover Re, RenaissanceRe, Swiss Re, SCOR and Willis Re. The Insurance Development Forum is also providing funding and input to accelerate finance-aware risk insight in developing markets.

Willis Towers Watson launched CyNat, a cyber insurance product designed for power and utility companies. The product seeks to offer a more tailored solution for companies in the sector that have significant potential for loss from attacks and are attractive targets due to their strategic importance.

Tokio Marine Holdings said it does not anticipate any material impact on its financials for the next fiscal year as a result of its relationship with Greensill Capital. The statement came in response to media coverage of Tokio Marine Holdings' subsidiary The Bond and Credit Company in Australia.

PIB Group acquired Acquinex, a specialist financial lines managing general agent. Formed in 2017 and headquartered in London, Acquinex specialises in providing mergers and acquisitions products, and underwrites warranty and indemnity and tax liability insurance for UK and European SME transactions. It has offices in Germany, Poland and Denmark.

Lloyd's went live with an earthquake policy which pays out within five days following a strong earthquake. The parametric policy has been developed in partnership with insurance start-up, Bounce, which tracks peak ground velocity data and then triggers policy payments when levels hit 20 centimetres per second and above.

Ecclesiastical Insurance posted a loss before tax of £15.7m (2019: profit before tax £73.3m) for the year ended 31st December 2021. This was driven by poor investment results. The group's gross written premiums grew 11% to £437m (2019: £394m) and in 2020 it returned a combined operating ratio of 95.1% (2019: 91.1%).

Specialist Risk Group recruited a 16-strong team from AFL Insurance Brokers with particular expertise in US, Canadian and Australian specialist wholesale, binding authorities and London Market facultative reinsurance. The team includes Jonathan Bines, who was previously CEO at AFL.

Value judgement

Amid the shift away from fossil fuels, the energy sector is undergoing rapid change, emphasising the need for asset owners, insurers and brokers to obtain accurate declared values. Deborah Ritchie spoke to CEO of John Foord, Andrew Slevin to understand the dynamics

Energy is an industry in transition as the world seeks to move away from fossil fuels and towards carbon neutral alternatives, in line with national agendas to reduce carbon emissions.

At the same time, insurers and re/insurers are increasingly hesitant to underwrite fossil fuel assets mainly driven by stakeholder pressure.

At the other end of the spectrum are maturing green energy technologies such as solar, hydrogen and wind that are seeing strong adoption. Innovation in green energy is driving down the costs of renewable energy assets and so insurers have been able to underwrite the risk for infrastructure, such as solar panels, at a lower premium cost.

Andrew Slevin, CEO of global specialist asset valuation and appraisal practice, John Foord, says all these factors put energy facility operators at risk of under and over-insurance scenarios.

Based in the firm's Singapore headquarters, Slevin manages a team of professionals across Australia, New Zealand, China, Thailand, Dubai, London and Singapore carrying out appraisals of over £70 billion of assets annually. In addition to setting valuation standards across John Foord, Slevin leads the valuation analytics division, driving innovation in appraisals solutions. With over 30 years' experience in asset valuations, he has worked on projects in over 50 countries.

What are the current challenges in insuring energy assets and how are they being addressed?

From our perspective as an independent valuer of assets in the energy industry, the challenge we are seeing is two-fold: rising costs to replace fossil fuel facilities combined with a growing reluctance among insurers to underwrite that risk, and on the other hand falling reinstatement costs to replace renewable energy assets and generally increased appetite among insurers to underwrite these projects.

One recent notable development, which may pose a slight headwind for some renewable energy assets, is extreme weather events such as hail, wildfires and flooding, which are leading to more claims from renewable facilities and thus driving up premiums in some cases.

However, our focus really remains on helping asset owners, insurers, brokers and financiers ensure that their sums insured are correct by providing them with accurate defendable declared values.

We have seen a rapid increase in reinstatement costs of fossil fuel assets and more decommissioning of facilities, with a similarly rapid reduction in associated costs of renewable energy assets.

Practically speaking, this means it is more important than ever for energy facility operators to have their declared values re-appraised and updated regularly to avoid both under and over-insurance scenarios.

In the former case (for fossil fuel assets), too little may be being paid in premiums and in the event of a claim the insurance pay out may not fully cover the current replacement costs at real market rates.

In the latter case (as with renewables), too much may be being paid in premiums and so savings can be made, or improved terms negotiated, by asset owners undertaking an appraisal and updating their declared costs.

How has the pandemic impacted requirements and challenges, and which changes are here to stay?

Due to pandemic-induced lockdowns and work from home implementations, it has been hard for asset owners to dedicate resources to ensure that values at risk have been carefully reviewed and updated.

As lockdowns are gradually lifted, this is unlikely to be a long-term challenge, but it does highlight a weakness in the insurance policy renewal process that needs to be addressed – determining current accurate values at risk can be time consuming and resource intensive.

Technology is proving to be a powerful solution, especially for facilities and assets that are not overly complex but have a risk and cost profile similar to hundreds or thousands of other sites around the world.

There may still be a need for a physical site survey by an expert valuer to determine correct current replacement costs with confidence for more complex projects and facilities, but site visits will be increasingly rare.

Andrew Slevin, CEO of John Foord

These new solutions are helping address challenges created by the pandemic and are offering new options to asset owners and insurers seeking to address the age-old problem of inaccurate sums insured.

Traditional, physical site appraisals will remain in demand in the industry, but they will exist alongside technology-driven solutions that offer clients increased real time insights into their portfolios.

Which specific technologies are being applied?

The traditional method for arriving at accurate reinstatement costs is to carry out a detailed site survey or on desk assessment. This approach has its benefits and is often the only viable approach for complex or unique locations.

Many asset owners and their advisors have more straightforward assets and want a simple way of quickly assessing whether values need more detailed analysis or whether current values are within an expected range.

We are in the process of building a cloud-based technology platform that give owners real-time access to accurate reinstatement costs by applying artificial intelligence and machine learning and powered by big data, including decades of previous assessments.

These specific technologies are applied to millions of data points on similar assets, helping to innovate on the valuation side of the insurance industry.

Leveraging the latest technology also ensures data integrity, cyber security, rapid response times and global scalability.

"Our focus is on helping asset owners and insurers to ensure that their sums insured are correct by providing them with accurate defendable declared values"

The upcoming John Foord Analytics platform offers three levels of accuracy based on the information provided to ensure that users can get an answer with the least possible inputs – but that they can also add additional information if a more accurate assessment is required.

We are integrating sophisticated proprietary modelling algorithms with decades of unique valuation and cost data to arrive at accurate and reliable reinstatement cost assessments.

John Foord has an established history, with its beginnings in London in the print sector. And it continues to evolve. What's on the horizon for the company?

We recognise that as a 200-year-old business, with a proud heritage and a record of excellence in the industry, we still need to keep up with new breakthroughs in technology to continue delivering value at scale to our global clients and partners.

As with many businesses around the world, the pandemic has acted as a catalyst for us to undertake a radical digital transformation of sorts as we have seen first-hand the challenges faced on the valuations side of the insurance industry.

So, the changes on the horizon for us as a company are all to do with cutting-edge technology and building out a competency that will hopefully see the John Foord brand continue to grow over the next two centuries.

John Foord is committed to delivering real industry value, creating significant change and disrupting the endemic under-insurance crisis across the insurance sector. We believe that by providing not just data but also credibility, improved insurance relationships and operational efficiency, our new technology platform will address existing valuation challenges that the insurance market has been struggling with in a rapidly evolving world.

Our ambition is to continue supporting insurers, advisors, financiers and asset owners who want to secure accurate and straightforward reinstatement costs that are delivered almost instantly.

Interview by Deborah Ritchie

Cyber insecurity

Phishing, viruses and ransomware are behind a surge in cyber breaches as workers headed home amid the pandemic, and fewer businesses put in place even basic security measures. Deborah Ritchie investigates

Two in five businesses have reported a cyber security breach or attack in the past 12 months, according to new government figures. Add this to the number of unreported attacks, and the National Cyber Security Centre's study is an indication that businesses are failing to take the necessary measures to thwart attacks.

The *Cyber Security Breaches Survey 2021* describes the extent to which the risk has heightened amid the pandemic, as organisational resources are diverted to facilitating home working, and the usual security measures are bypassed.

According to the data, the most common breaches or attacks were phishing emails, followed by viruses or other malware.

The study shows that fewer businesses are using security monitoring tools to identify abnormal activity that could indicate a breach, which suggests firms are less aware than before of breaches and attacks. The number of businesses with up-to-date anti-virus software is also down from the previous year, at 83 per cent.

The figures also reveal nearly half of businesses have staff using personal devices for work, but only 18 per cent have a cyber security policy on how to use those personal devices for business purposes.

Perhaps most significantly, fewer than 23 per cent of the businesses polled have a cyber security policy covering home working.

Despite all this, businesses report that cyber security is a high priority; 77 per cent said it was key, up 12 per cent from the 2016 report.

It is clear that there is a disconnect

between good intentions and what is actually happening on the ground – suggesting a genuine need for greater resilience in cyberspace.

Commenting on the findings, digital infrastructure minister Matt Warman said: “The pandemic has taken an unavoidable toll on British businesses but we cannot let it disrupt our high cyber security standards.

“With more people working remotely it is vital firms have the right protections in place, and I urge all organisations to follow the National Cyber Security Centre’s expert guidance so we can build back better and drive a new era of digital growth.”

DCMS says it is reviewing what more the government can do to improve businesses’ resilience, and has committed to publishing a new National Cyber Strategy later this year.

Meantime, work is progressing on new legislation that secure smart devices by ensuring that makers of phones, speakers and doorbells tell customers upfront how long a product will be guaranteed to receive vital security updates, among other measures.

These moves have been supported by tech associations across the globe, including the Internet of Secure Things (or IoXT), whose members include some of the world’s biggest tech companies including Google, Amazon and Facebook.

Brad Ree, CTO of the IoXT Alliance, says: “We applaud the UK government for taking this critical step to demand more from IoT device manufacturers and to better protect the consumers and businesses that use them.

“Requiring unique passwords, operating a vulnerability disclosure programme, and informing consumers on the length of time products will be supported is a minimum that any manufacturer should provide. These are all included in the IoXt compliance programme and have been well received by manufacturers around the world.

“The new law builds upon world-leading work the government has already done to boost the security of smart devices, including publishing

“The pandemic has taken an unavoidable toll on British businesses but we cannot let it disrupt our high cyber security standards”

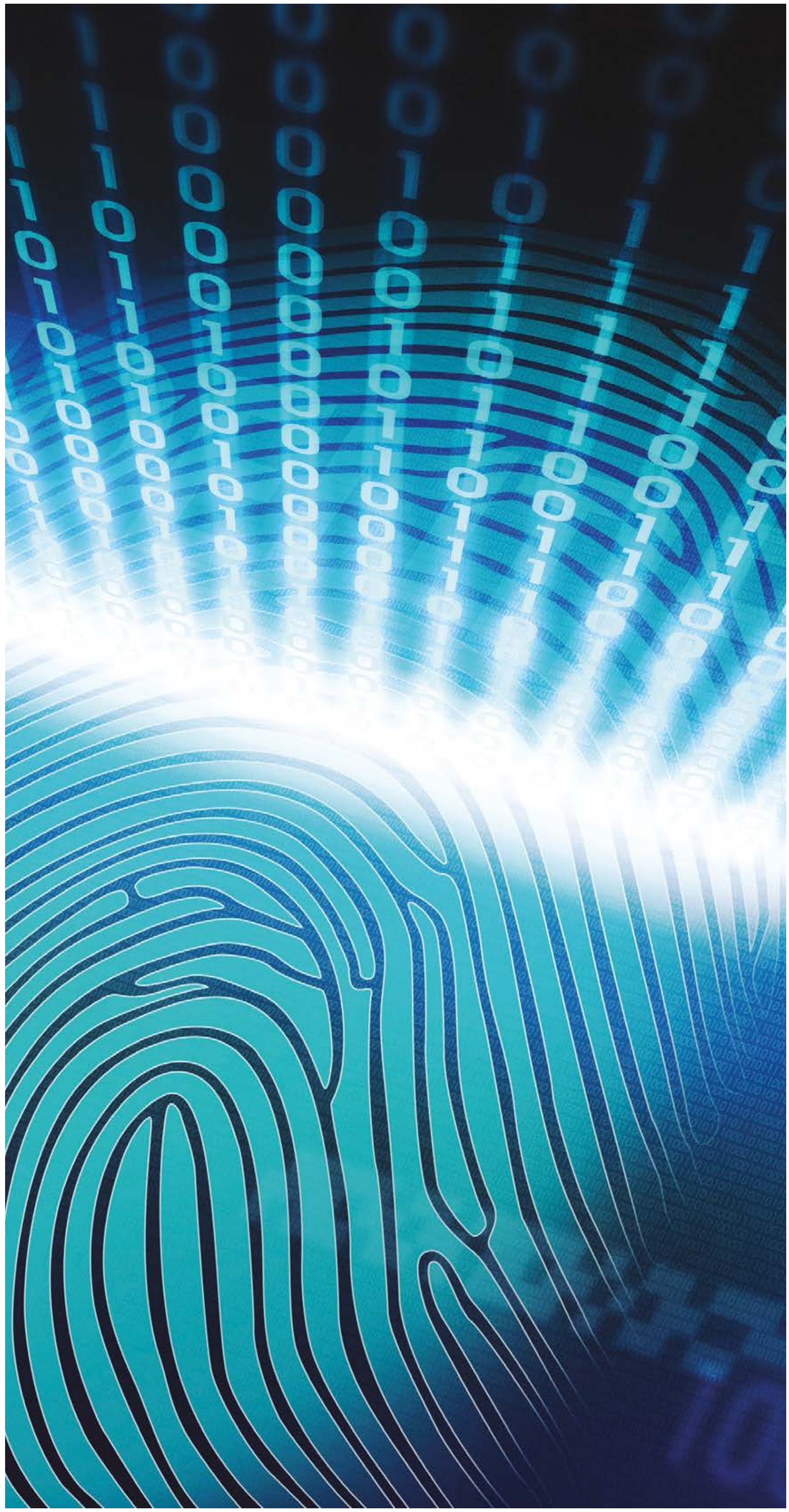
Rank	Police Force	Total Number of Cyber crimes	Population (2019)	Cyber crimes per 100,000 people
1	Metropolitan	5,934	8,952,300	66.3
2	Hertfordshire	749	1,189,500	63.0
3	Wiltshire	425	722,200	58.8
3	Kent	1,094	1,860,100	58.8
5	Surrey	698	1,196,200	58.4
6	Dorset	444	773,800	57.4
7	Cheshire	605	1,066,600	56.7
8	Warwickshire	320	577,900	55.4
9	Thames Valley	1,333	2,420,000	55.1
10	Hampshire	1,062	1,991,700	53.3

The UK areas with the highest rate of cyber crime (Source: ESET)

Rank	Area	Cyber crimes reported in Jan 2020	Cyber crimes reported in Jan 2021	YoY Increase	YoY Increase (%)
1	Police Scotland	9	27	18	200.0%
2	Cheshire	34	57	23	67.6%
3	Surrey	34	56	22	64.7%
4	Wiltshire	26	42	16	61.5%
5	Cumbria	12	18	6	50.0%
5	Gwent	8	12	4	50.0%
7	Lincolnshire	26	38	12	46.2%
8	North Yorkshire	24	33	11	45.8%
9	Cambridgeshire	25	35	10	40.0%
10	PSNI	30	41	11	36.7 per cent

The UK areas with the biggest increase in cyber crime (Source: ESET)

"The most commonly provided products and services include cyber professional services, threat intelligence, monitoring, detection and analysis, with major growth areas identified in industrial control systems and IoT security"



a code of practice for device manufacturers to boost the security of their products in 2018.

John Moor, managing director of the Internet of Things Security Foundation, adds: "We welcome this announcement as a necessary and considered development to make consumers safer. As an expert body, we welcome the clarity it brings for our manufacturing members both now and moving forward.

"The internet of things is constantly evolving and security requirements must continue to keep pace. As such, the importance of vulnerability management and updating security software cannot be understated. In the words of one of our members: 'remember, if it ain't secure, it ain't smart.'"

The NCSC's study makes for sobering reading, but perhaps not entirely surprising. We have all seen the reports of increased cyber crime amid the pandemic. What is perhaps less widely reported is where instances of cyber crimes against people are most prevalent.

A recent ESET study suggests an increase of cyber crimes across the UK of over 19 per cent, with London the worst affected.

ESET's *UK Cybercrime Report* found around three-quarters of reported cyber crimes in the UK fell under 'hacking', with just under a quarter involving the installation of computer viruses, malware and spyware.

Commenting on the study Jake Moore, cyber security specialist at ESET, said: "What is initially apparent is that there has been a nationwide increase and cyber criminals will pursue the data rather than target people specifically. However, knowledge is the key to reducing cyber crime and where this data has highlighted inevitable increases, it may suggest those areas are lacking in cyber security awareness and a focus on education is now necessary."

MS Exchange attacks could lead to thousands of insurance claims

Insurers are being warned of the potential for a large volume of claims following recent cyber attacks on Microsoft's email servers.

Tens of thousands of Microsoft Exchange servers in businesses and organisations around the world could have been infected during a series of concerted attacks since the beginning of this year.

Cyber analytics specialists at CyberCube believe companies in North America to be at greater risk than those in Europe, but large to medium-sized businesses globally are all vulnerable. It says that the insurance and reinsurance industries are "likely to see a long-tail of attritional claims resulting from this attack".

William Altman, cyber security consultant at the firm, says: "The insurance industry is only just beginning to understand the scope of possible damage. It is too early to calculate potential losses from the theft of a corporation's intellectual property. These kinds of data breaches could have delayed - but long-lasting - impacts on commercial competitiveness.

"An accumulation of loss could result in multiple – theoretically, tens of thousands – of companies making insurance claims to cover investigation, legal, business interruption and possible regulatory fines. There is still the ongoing possibility that even more attackers will launch ransomware or other types of destructive cyber attacks."

Researchers believe that 10 different "advanced persistent threat actors" globally are now actively exploiting the code used in this attack in a variety of ways. Microsoft has provided patches for the vulnerabilities, but attackers seem to have stepped up their efforts to identify unpatched servers.

Record year for sector investment

Despite the pandemic (or because of it?) the UK's cyber industry attracted record investment last year.

New analysis suggest that almost 50,000 people are now employed in UK cyber security, with the number of active cyber security firms in the UK up 21 per cent on last year. The sector contributed more than £4 billion to the economy, attracting some £800 million of investment. The sector is now worth an estimated £8.9 billion, according to the Government's annual *Cyber Sector Report*.

Tracking the UK's cyber security industry across a range of indicators between April 2019 and December 2020, the report suggests there are 1,483 operating in the field, employing a total 46,683 people – 65 per cent of whom are employed by large firms. The most commonly provided products and services include cyber professional services, threat intelligence, monitoring and detection and analysis, with major growth areas identified in industrial control systems and IoT security – a signal, the report's author's believe, points to the sector's adaptation towards such emerging challenges as the need to secure smart cities. These won't just be in the capital, as this year's survey also suggests that more than half of these firms are now based outside of London and the South East, with clusters of activity proliferating in Scotland, Northern Ireland and North West England, among others.

"Half of businesses have staff using personal devices for work, but only 18 per cent have a cyber security policy in place for that"

UK start-ups in the sector have received some £1.25 billion in government support throughout the pandemic, with programmes such as the LORCA cyber accelerator and the NCSC Accelerator playing a part in supporting innovation. Meanwhile, the DCMS-funded CyberASAP programme supports the commercialisation of cyber security research from UK universities.

Julian David, chief executive officer of techUK says reliable cyber security is essential for all organisations as they accelerate digital transformation in the wake of ongoing COVID-19 disruption.

"This research shows a sector going from strength to strength, with increasing investment in our growing cyber ecosystem and, perhaps most significantly, uptake of the technologies and services keeping UK citizens and business safe.

"One key finding is that 54 per cent of cyber companies are now based outside London and the South-East, an encouraging change which will improve cyber resilience across all the nations and regions of the UK, as well as sharing the economic prosperity offered by this fast-growing sector. This regional development is one area which techUK will continue to actively partner with DCMS, through initiatives like Cyber Exchange, as government and industry continue to strengthen the UK's position as a leading cyber nation."

Deborah Ritchie is editor of CIR

Taking the hybrid road

A hybrid working approach seems to be the way forward for businesses that have the option, although many employers are yet to determine how this will work in practice. Deborah Ritchie reports

Over a year has passed since the coronavirus pandemic was declared, forcing companies to adopt new working practices to ensure business continuity. Now, as restrictions begin to ease again and businesses consider their new normal after many months with swathes of the workforce working from home, questions about how a hybrid working approach will work in practice need addressing.

As the UK's vaccination programme got underway at the beginning of the year, opinions around the 'new normal' began to emerge, with business group Resilience First warning office-based firms not to plan for full occupancy – urging business leaders to accept that any return to the office would be a hybrid one. Meanwhile, HSBC announced plans to almost halve its global office footprint, and AXA offered employees the option to work remotely two days per week. At the same time, Goldman Sachs CEO David Solomon said he wanted all his people back in the office.

The speed and extent of the return to offices and cities was addressed by Prime Minister Boris Johnson when he said (at a virtual Network Rail conference) that commuting would be back "in a few short months" and that the current WFH approach was "a temporary thing".

Fast forward two months, and Johnson may have misread the signs, as – for now at least – they are clearly pointing in the opposite direction.

A new Institute of Directors survey of around 600 business leaders (conducted in March, and excluding businesses that have always worked from home) has shown that over 60 per cent of organisations plan to adopt hybrid working even after restrictions ease. Respondents to the survey signalled an intent to shift towards

A blended approach

Which of the following most closely describes your organisation's expected average use of the 'workplace' in the long-term? 'Workplace' can refer to offices, factories and workspaces other than home working.

No remote working	19 per cent
1 day per week remote working	11 per cent
2 days per week remote working	24 per cent
3 days per week remote working	20 per cent
4 days per week remote working	8 per cent
Fully remote working	11 per cent
Don't know	6 per cent

On balance, do you find remote working more or less productive for your own work?

Significantly more productive	11 per cent
Slightly more productive	29 per cent
No change	20 per cent
Slightly less productive	27 per cent
Significantly less productive	10 per cent
Remote working is not suitable for my work	4 per cent

Source: Institute of Directors

one to four days of remote working per week, and one in ten are now looking to work from home entirely. Only a fifth were not planning to introduce any form of remote working.

A large number of employers said they felt that working from home was more productive for staff – although there was a significant enough percentage that did not to suggest that a hybrid working model was most likely to provide the optimum balance.

"As the economy reopens, business leaders are grappling with the best working models going forward," says Joe Fitzsimons, senior policy advisor at the IoD. "The flexibility of remote working has improved work-life balance for employees and cut-down commuting expenses. In many cases it has also boosted inclusivity and hiring from different parts of the country.

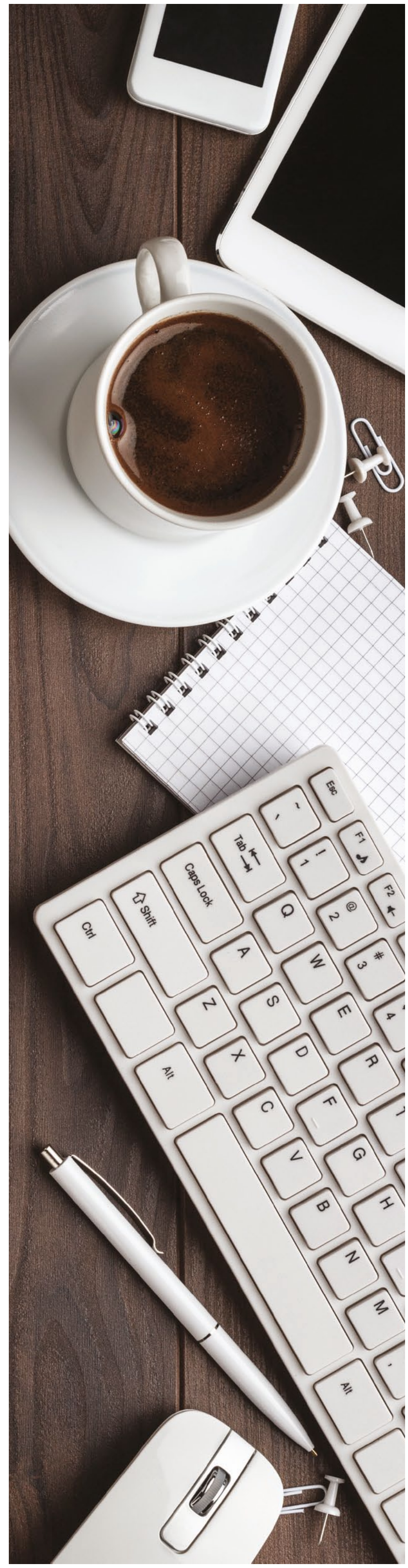
"Despite the advantages, remote working has not been without its challenges. For business leaders, running a tight ship has not been easy without workforces in the same physical space. This is not helped by unreliable internet connections."

Clearly, for organisations that require customer interaction, remote working is less suitable. However, many firms are also looking to cut back on office sizes, amp up home working, and make more use of co-working spaces, according to the study, which suggests that directors are working with employees to find the most productive working arrangements to suit varied preferences and different business models.

Making flexible work

The issue of cyber security risks emanating through staff working from home is one that firms are increasingly aware of, if not yet on top of (see our cover story on page 16 for more on that) but there are other issues when it comes to safeguarding staff that work from home.

The Association of British Insurers is hoping to harness the changing expectations in the transition to post-pandemic life to improve gender equality in the insurance industry by giving both men and women the power to work flexibly. A total of 27 firms have signed the association's



Making Flexible Work charter, its key aim to attract and retain the best talent from all backgrounds to the sector. Signatories range from Allianz and Aviva to Zurich.

Yvonne Braun, executive sponsor for diversity and inclusion at the ABI, says: "[This] announcement represents one of the biggest ever commitments to increasing flexible working in financial services. By joining the Making Flexible Work campaign, firms will tackle the gender seniority gap and be able to attract and retain the brightest and best talent in our industry.

Amanda Blanc, group CEO at Aviva and HM Treasury's Women in Finance Champion, adds: "There are still too many barriers which stop women progressing in insurance. As an industry we need to do more, and do it quicker, to make the changes we all want to see. Flexible ways of working is one way, but it needs to be available to everyone.

"The pandemic has shown us the value of flexible working, but to truly level the playing field at the office and at home, both men and women should feel able to work flexibly."

Staying with inclusivity, one firm of business psychologists is urging leaders to consider the potential discrimination and diversity issues that it says could be caused by poorly planned hybrid working approaches.

Cambridge-based consultant OE Cam says employers must be careful to ensure that "women, the disabled, parents, older workers and culturally diverse employees have equal opportunities in the workplace".

The formation of 'in-groups' and 'out-groups' will be even more prominent in a hybrid workforce, it says, adding that 'present privilege' means that those in the workplace are "more likely to be involved in spontaneous discussions in the office and have better access to the boss… [and] that promotion".

"The issue for any organisation now is to reduce the effects of out-groups. Businesses must be mindful of which employees are the ones most likely to wish to work remotely most of the time," explains Martyn Sakol, managing partner at OE Cam. "Experts believe that there are certain groups this will include: those with caring responsibilities, parents (with more mums choosing, or even feeling obliged, to work remotely over dads), disabled employees – for whom the commute can be more difficult – and older generation workers, hoping to improve their work-life balance.

"To prevent these staff from losing their voice, their ability to contribute effectively to the business and their chance of promotion, firms must take active steps. This is not something that will just 'work itself out' as teams become accustomed to hybrid working."

It's clear that a hybrid approach to work can bring huge advantages, but making it work will require careful consideration of all the risks.

Deborah Ritchie is editor of CIR

Insurers' post-pandemic working wishlist

A social media survey of Chartered Insurance Institute members showed half expect to work remotely two to three days a week, once the government's guidance to slow the spread of coronavirus changes, to allow greater access to the office.

One in five of the 3,902 individuals who took part in the poll expect to spend the bulk of their week in the office and no more than one day a week working remotely once they are safely able to do so.

The same amount of insurance professionals stated once the government guidance to work from home if you can changes, they still intend to stay away from the office for the bulk of the working week and spend at least three to four days a week remotely and only one to two days physically alongside colleagues in the office.

Just one in 10 of the thousands of insurance professionals who took part in the CII's poll stated they intend to go fully back into the office five days a week once the government guidance changes.

According to current government guidance, office workers should currently work from home if they can.

This guidance will remain in place until at least Step 4 of the government's roadmap, which is currently scheduled for no earlier than 21st June, when the work from home guidance will be considered as part of the wider review on social distancing.

Commenting on the poll, Jodie Horgan, group sales and marketing director of Clear Insurance Management, says: "There is a lot more want and need to be in the office compared with a year ago when I did hear a lot of people never wanting to go back.

"I, for one, am looking forward to having the option to go back again."

Varsha Parmar, insurance adviser at BrokerLink, says: "[The] best thing about COVID-19 has been working from home. I actually have a better work-life balance now that I am working from home."

Keith Richards, chief membership officer of the Chartered Insurance Institute, adds: "The virus broke through cultural and technological barriers that prevented greater remote working in the past. The results of this survey show the limitations and benefits of remote working have been made clear by the COVID-19 pandemic.

"Clearly one size does not fit all when it comes to identifying how insurance professionals wish to work once government guidance on working from home changes.

There is clearly an appetite for greater remote working to persist post pandemic. Insurance professionals must now figure out what works best remotely and what tasks require personal interaction in order to deliver the best outcomes for consumers."

Feeling the heat

The consequences of climate change, including the transition itself, are changing risk and operating environments. As COP 26 approaches, Deborah Ritchie examines the issues

Global emissions must halve by 2030 to keep global warming below 1.5 degrees, and with over 110 countries committed to becoming carbon neutral by 2025, it is hoped that this year's United Nations COP 26 climate change summit will set the pace for defining and strengthening policy response. Whether or not the physical event will go ahead as planned hangs in the balance, but whatever form the summit takes (and if the past 18 months have shown us anything, it is that the world does not stop turning when we meet remotely), tackling climate change at the global level is front of mind – something the pandemic has served to underline with the emphasis now a united green recovery from coronavirus, which creates sustainable jobs and addresses the urgent and linked challenges of climate change and public health, building on the original commitments made in 2015 as part of the Paris Agreement.

According to Swiss Re Institute research, climate change poses the biggest long-term risk to the global economy. By the middle of the century, the world stands to lose around 10 per cent of total economic value from climate change. That, the organisation insists, is a real scenario if temperature increases stay on the current trajectory, and both the

"Research suggests that if temperature increases stay on the current trajectory, the world stands to lose around 10 per cent of total economic value by the middle of the century"

Firms back new climate networks

More than 600 businesses, with annual revenues of more than £2 trillion and employing more than 10 million people across 150 countries, are joining a new collaboration between think tank, The Resilience Shift and Resilience First.

The new network brings together disparate industries – from finance, to retail, technology, engineering and the built environment – to help governments and businesses promote economic recovery and shape post-pandemic stimulus that builds resilience and accelerates global decarbonisation efforts.

"The next five years are critical to the future of our planet and resilience will be central to helping us survive and thrive," says Seth Schultz, executive director of The Resilience Shift. "We need to be able to withstand and adapt to changing conditions and recover positively from shocks and stresses. [This] announcement is the beginning of many radical shifts that will more appropriately prepare us to meet the challenges of the coming decade. We invite organisations to join us in our mission for a more resilient world".

Businesses involved include Arup, WSP, Dar Group, NBC Universal International, Tesco, Intel and the Lloyd's Register Foundation.

Dame Jo da Silva, global sustainable development leader at Arup, says: "Over the last year, the importance of resilience has been made starkly clear; from firms enabling us all to adapt to online work or adapting to online products and services, through to healthcare services responding to the massive increase in intensive care cases, and even energy and transport networks operating on a skeleton staff.

"This ability to adapt to and recover from crisis or change will only become more critical as we navigate the implications of climate change, digital transformation, a growing population and less resources over the next 20 years."

The collaboration is just one of a number of alliances to have sprung up in recent years to lead climate initiatives.

On the eve of President Biden's Head of State Climate Summit, a new global alliance that brings together existing and new net-zero finance initiatives into one sector-wide strategic forum was launched. The Glasgow Financial Alliance for Net Zero, chaired by Mark Carney, UN Special Envoy on Climate Action and Finance, unites over 160 firms (together responsible for assets in excess of US$70 trillion) from the leading net-zero initiatives across the financial system to accelerate the transition to net-zero emissions by 2050.

Meanwhile, 43 banks have collaborated to form the UN-convened Net-Zero Banking Alliance. The new banking initiative becomes a founding member of the GFANZ alongside the Net-Zero Asset Owner Alliance. The NZBA joins three existing initiatives: the Net-Zero Asset Owner Alliance, the Net Zero Asset Managers Initiative and the Paris Aligned Investor Initiative.

Separately, some of the world's leading insurers and reinsurers, are establishing the Net-Zero Insurance Alliance under the auspices of UNEP FI's Principles for Sustainable Insurance, building on their climate leadership as investors via the UN's Net-Zero Asset Owner Alliance. The seven companies involved in establishing the NZIA are AXA (chair), Allianz, Aviva, Munich Re, SCOR, Swiss Re and Zurich Insurance. The NZIA has submitted a statement of intent to join the UN Race to Zero and become part of the GFANZ and is expected to be officially launched at COP26.

UK Prime Minister, Boris Johnson, said: "Uniting the world's banks and financial institutions behind the global transition to net-zero is crucial to unlocking the finance we need to get there – from backing pioneering firms and new technologies to building resilient economies around the world. The Glasgow Financial Alliance for Net Zero will lead this charge ahead of COP 26 to scale-up our ambition, accelerate our shift and help us to build back greener together."

Mark Evans is editor of the Better Society Network

Paris Agreement and 2050 net-zero emissions targets are not met.

Economies in South and South East Asia are the most vulnerable to the physical risks associated with climate change (including Malaysia, Thailand, India, the Philippines and Indonesia); they also have the most to gain if the world is able to rein in temperature increases. Advanced economies in the northern hemisphere (including the US, Canada, Switzerland and Germany) are less vulnerable, being both less exposed to adverse developments in weather patterns associated with climate change, and better resourced to cope.

Climate change also poses transition risks, such as large shifts in asset values and higher costs of doing business as the world moves to a low-carbon economy. Once again Asia is likely to be the most heavily affected. And, as global warming makes the impact of weather-related natural disasters more severe, it can lead to substantial income and productivity losses over time, such as loss of land resulting from rising sea levels, and crop failures resulting from heat stress. The Swiss Re Institute conducted a stress test to examine how 48 economies would be impacted by the ongoing effects of climate change under four different temperature increase scenarios Expected global GDP impact by 2050 under different scenarios compared with a world without climate change are:

- -18% if no mitigating actions are taken (3.2°C increase);
- -14% if some mitigating actions are taken (2.6°C increase);
- -11% if further mitigating actions are taken (2°C increase);
- -4% if Paris Agreement targets are met (below 2°C increase)

In a severe scenario of a 3.2°C temperature increase, the findings suggest that China stands to lose almost one quarter of its GDP (24 per cent) by mid-century. The US, Canada and the UK would all see around a 10 per cent loss. Europe would suffer slightly more (11 per cent), while economies such as Finland or Switzerland are less exposed (6 per cent) than, for example, France or Greece (13 per cent).

Thierry Léger, group chief underwriting officer and chairman of the Swiss Re Institute, says: "Climate risk affects every society, every company and every individual. By 2050, the world population will grow to almost 10 billion people, especially in regions most impacted by climate change. So, we must act now to mitigate the risks and to reach net-zero targets. Equally, as our recent biodiversity index shows, nature and ecosystem services provide huge economic benefits but are under intense threat. That's why climate change and biodiversity loss are twin challenges that we need to tackle as a global community to maintain a healthy economy and a sustainable future."

Given the long-term horizon of their liabilities and long-term capital to commit, institutional investors, including insurance companies, are ideally positioned to play a strong role.

Swiss Re's group chief economist, Jérôme Haegeli, says climate change is a systemic risk which can only be addressed globally. "So far, too little is being done. Transparency and disclosure of embedded net-zero efforts by governments and the private sector alike are crucial. Only if the public and private sectors pull together will the transition to a low-carbon economy be possible. Global cooperation to facilitate financial flows to vulnerable economies is essential. We have an opportunity to correct the course now and construct a world that will be greener, more sustainable and more resilient.

"Economies in South and South East Asia are the most vulnerable to the physical risks associated with climate change; they also have the most to gain if the world is able to rein in temperature increases"

In numbers: The UK, host of the 2021 COP26 Summit

The first major economy to pass laws for net zero carbon emissions by 2050, the UK is the fastest country in the G20 to decarbonise its economy since 2000, and has cut emissions by more than 40 per cent since 1990 – the fastest rate in the G7.

The UK is also the largest producer of offshore wind energy in the world, and has a low carbon economy that is predicted to grow four times faster than the rest of the economy to 2030.

The country's expertise and exports are in demand across the world, with global trade in low-carbon goods and services expected to grow from £150 billion in 2015 to between £2.8-£5.1 trillion in 2050.

"Our analysis shows the benefit of investing in a net-zero economy. For example, adding just 10 per cent to the US$6.3 trillion of annual global infrastructure investments would limit the average temperature increase to below 2°C. This is just a fraction of the loss in global GDP that we face if we don't take appropriate action."

Whether it is the global pandemic, the work of the Biden Administration, or UK Prime Minister Boris Johnson's recent interest in the subject, there is a renewed sense of urgency in the climate change conversation.

Companies everywhere are beginning to recognise the threat posed by climate change to all aspects of their business – beyond the obvious damage caused to the planet.

In the view of city law firm Clyde & Co, it is not so much carrot as stick behind the shift in consciousness. Partner at the firm, Nigel Brook observes an increase in high-profile litigation resulting in significant losses for businesses, as climate-related risks become more prevalent.

"At Clyde & Co, we believe a proactive, rather than reactive, approach to the new risk environment is sensible, drawing on good governance and turning it into action. It represents an opportunity for businesses to build resilience against climate risk and transition to a new, and better, way of operating."

Launching its 2021 Climate change risk and liability report, *Stepping up Good Governance to Seize Opportunities and Reduce Exposure*, the law firm says the conversation at an organisational level has changed in the two years since it began the study when climate change was still a relatively nascent boardroom issue for businesses outside the energy sector.

As this issue of the magazine goes to print, concerns over how to host the COP 26 event with social distancing, international travel, varying levels of COVID immunity and infection rates globally is creating a logistical challenge, despite the Government, and COP 26 president Alok Sharma being keen to host a physical event. At the same time, there is a sense that the pandemic has created a window of opportunity for change – something that appeals to activists and politicians in equal measure.

Access the Clyde & Co report here: https://www.clydeco.com/en/reports/2021/3/climate-change-risk-and-liability-report-2021

Deborah Ritchie is editor of CIR

The tempest threatens

From a failure to put in place robust IT or health systems, to being accused of mishandling their firms' responses to the pandemic or to climate change, boards face a vast and expanding array of costly liabilities. Deborah Ritchie reports

The past 18 months have brought a great many risks to the fore, and with them, some considerable shifts in perception of the potential liabilities facing company directors and officers.

From a failure to have robust IT systems in place and inadequate handling of increased exposure to cyber risks, to occupational health breaches or even corporate manslaughter accusations resulting from a failure to ensure adequate health and safety in the workplace, the risks are many and varied, and often in uncharted territory. And in an ESG-conscious world, the responsibility remit is ever widening. Directors and officers must now ensure robust, resilient, sustainable and profitable business models, whilst guaranteeing the welfare and safety of their people, their customers, the environment and society as a whole.

That boards have a huge task on their hands to navigate this broad range of risks is in no doubt. As Willis Towers Watson's April *D&O Liability Survey* shows, the highest rated risks perceived by directors and officers across the finance and insurance, industrial and manufacturing, services, hotels and leisure, wholesale, retail and consumer goods, TMT, real estate, life sciences, and infrastructure industries continue to be cyber attack and data loss (in the top two for the last three years).

"Given the prevalence of cyber crime and the severe consequences for companies and [directors and officers] should they fall foul of an attack and/or data is lost, this is no surprise," the report reads. "The COVID-19 pandemic has proved to be a fertile ground for cyber criminals seeking to exploit the weaknesses presented by businesses to move to new procedures and systems overnight, often with a remote workforce. The trend is towards bigger targets and bigger incidences, and ransomware attacks are also on the increase, which could expose [directors and officers] to criminal sanctions for breaches of terrorism and proceeds of crime laws."

Geographical nuances

In Australia, an increasing prevalence of ransomware, state-sponsored cyber attacks and increasingly sophisticated and directed method of attacks has considerably increased the risk for corporates. It has also provoked hyperactivity from APAC regulators, with directors and officers directly targeted by the watchdog. Similar privacy reforms have either recently been implemented or are on the agenda in Japan, Singapore and New Zealand. "By comparison with some of the other regions, regulatory risk continues to be a high priority risk in the APAC region ranking second in the top five. In Australia, corporate regulators, including the

Understanding cover

Specialist insurance broker, McGill and Partners recently warned that directors and officers could face significant legal expenses and other liabilities, running into the millions, due to a misunderstanding of the way in which their cover works.

Its survey of more than 100 board members in the UK found that just 17 per cent understood whether they would be covered for a claim made against them after they left the company, based on allegations of misconduct whilst in office, and that 83 per cent failed to appreciate that such protection could not be guaranteed if the company did not continue to purchase appropriate D&O insurance after they had left.

The same study found that just 21 per cent understood that the D&O policy might not cover them for all their legal representation costs in the event of the company's insolvency.

Commenting on the findings, Francis Kean, partner in McGill and Partners' financial lines team says: "Many directors don't understand how their cover will be affected by changes to the company. Events completely outside of directors' control can restrict or curtail the cover available to them. This means that many could be leaving themselves open to serious financial losses, and even bankruptcy, by not understanding the nature and limitations of their cover.

"With a D&O insurance programme it may be that the recipients of the cover aren't necessarily involved in the purchasing which could be one reason behind the knowledge gap. Unless there is a stronger connection between the product and its intended end users there is the very real risk of serious expectation gaps, or worse, emerging at the worst possible time."

Australian Securities and Investments Commission, have continued to pursue the 'why not litigate' approach (a legacy of its criticism following the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, completed in 2019) and enforcement actions generally are increasing," the report states.

While regulatory and litigation risk and shareholder claims have fallen below the top five risks, each have the potential to trigger regulatory investigations (which are increasingly being brought by more aggressive regulators) and follow-on civil claims, as well as shareholder litigation against the board of directors.

Insurers also report concerns that corporate or financial restructuring, job losses and insolvencies could trigger investigations into directors' conduct and then transcend into D&O claims. There is also an increased focus on analysing corporate governance and assessing how boards are managing risks during the pandemic.

In the US, a particularly high perception of risk ranks employment claims considerably higher at just over 45 per cent (making it joint third highest risk for respondents in the US) when compared to the global result which ranked employment claims as fifth, with 38 per cent.

"Employment claims have long been a substantial business risk, with high-frequency claims and, in some cases, very high-severity claims

"Insurers report concerns that corporate or financial restructuring, job losses and insolvencies could trigger investigations into directors' conduct and then transcend into D&O claims"

Top 5 risks to businesses

Rank	2021	2019	2018	2017	2016	2014	2013	2011
#1	Cyber-attack	Data loss	Risk of data loss / data breach	Regulatory and other investigations	Regulatory and other investigations and inquires	Regulatory and other investigations and inquires	Regulatory and other investigations and inquires	Regulatory and other investigations and inquires
#2	Data loss	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Anti-Corruption Legislation (including the Bribery Act)	Criminal and regulatory fines and penalties	Criminal and regulatory fines and penalties
#3	Regulatory risk (including threat of fines and penalties)	Regulatory risk (including threat of fines and penalties)	Regulatory and other investigations	Risk of data loss / data breach	Risk of data loss / data breach	Criminal and regulatory fines and penalties	Anti-Corruption Legislation (including the Bribery Act)	Anti-Corruption Legislation (including the Bribery Act)
#4	Health & safety / environmental prosecutions	Litigation risk	Health and safety legislation	Criminal and regulatory fines and penalties	Criminal and regulatory fines and penalties	Risk of being sued abroad	Securities / Shareholder claims	Employment practices claims
#5	Risk of employment claims	Social media campaigns	Criminal and regulatory fines and penalties	Concerns in a post Brexit landscape	Anti-Corruption Legislation (including the Bribery Act)	Multiplicity of sanctions regimes and of affected countries	Risk of being sued abroad	Securities / Shareholder claims

Top five risks to business, ranked based on percentage "very important" or "extremely important" for each risk
Source: Willis Towers Watson Directors & Officers Liability Insurance Surveys

impacting operations – with select matters (such as #MeToo) shaking up the C-suite itself," the report states. "It is perhaps not surprising that exposures relating to pandemic-triggered furloughs and layoffs, as well as return to work and vaccination policies, may exacerbate those concerns, bringing these issues higher into the top five, in the minds of our US respondents."

Corporate accountability directive heaps pressure on directors

Henning Schaloske, partner, Clyde and Co Dusseldorf; and Simon Konsta, partner, Clyde & Co London

Under a new corporate accountability directive due to be submitted by the end of this year, companies operating in the EU will face new reporting requirements regarding environmental and human rights standards within their international supply chain from the beginning of 2022.

The EU Corporate Due Diligence and Corporate Accountability Directive is the latest evidence of the growing trend for environmental issues to be considered through the lens of human rights as companies are increasingly held to account for ensuring that their actions, and those of their suppliers, serve to protect and safeguard the environment for the benefit of future generations.

In the UK, European, Canadian and Australian courts, 2020 was marked by a notable increase in human rights environmental cases with more than 1,500 claims filed in 38 countries by mid-2020, up from fewer than 900 in 24 countries in 2017, according to the UN Environment Programme. In the past three years, the number of instructions received by specialist climate teams at Clyde & Co offices as far afield as London, Europe and the US has more than doubled.

The new directive will place broader obligations on companies that will be reflected in domestic and European legislation. This is expected to add further to the pressure on directors and officers to gain greater control of their supply chains and is likely to prove particularly challenging for larger businesses and those with complex multinational supply networks.

The key elements of the proposed directive are:

- Due diligence will be required so companies can identify, address and remedy their impact on human rights and the environment throughout their value chain
- Rules will apply to all companies operating in the EU internal market, including those from outside the EU
- Sanctions will be imposed for non-compliance of environmental standards
- Damages by injured third parties will be in the scope of this legislation, going beyond current plans for a Supply Chain Act in Germany

"In a world of increasingly accessible litigation funding and an ever more sophisticated claimant bar, consistent, accurate reporting around climate, sustainability and ESG promises has never been more important"

"As they prepare to comply with the mounting reporting requirements of new regulations around supply chains, directors will also need to keep in mind that scrutiny over perceived greenwashing is increasing"

It is anticipated that fines and sanctions to be brought in under the new directive may follow the model adopted by the GDPR Directive. That being the case, fines would be calculated as a percentage of global turnover. This could mean substantial penalties – particularly for larger businesses with complex global supply chains.

Important questions will include the insurability of fines or whether and to what extent companies might seek recourse from their D&Os, and, if so, how D&O insurance policies respond to such claims. Re/insurers are keen to work on responses to notifications and are starting to think about the position they will want to take as potential liabilities and losses rise.

Insurers have already taken steps to remediate D&O portfolios by raising rates, reducing limits and tightening wordings, but of course, the EU is not the only body planning new regulations in this space. In a related development, the UK Government launched in March a consultation on wholesale reform of UK audit and corporate governance. One of the proposals concerned the mandating of a new Resilience Statement in company reports that might, amongst other areas, be required to report upon risks such as supply chain resilience and climate change.

Greenwashing risk

As they prepare to comply with the mounting reporting requirements of new regulations around supply chains, directors will also need to keep in mind that scrutiny over perceived greenwashing is increasing. Internal and external stakeholders alike are keen to know how reliable businesses' green statements are – not just in regard to supply chain but indeed any aspect of their operations.

Such issues were brought into sharp relief last year by the €5 million fine imposed on Italian energy giant ENI by the country's Competition and Markets Authority over claims that its diesel containing 15 per cent treated palm oil was green, despite the fact that palm oil production is a well-known cause of deforestation. At this time of mounting consumer expectation and protection, ESG misstatements of this kind constitute a legal and reputational vulnerability.

In a world of increasingly accessible litigation funding and an ever more sophisticated claimant bar with access to collective consumer redress remedies and class actions, consistent, accurate reporting around climate, sustainability and ESG promises has never been more important.

Climate of opinion is shifting

Discussion of the new requirements, which are intended to set new standards for responsible business conduct in Europe and beyond, has drawn emotive comments from international MEPs who spoke of the need to "take back control against these global multinationals that think they are above the law".

Such comments suggest a less favourable climate of opinion among stakeholders moving forward, raising the stakes ever higher for directors and officers and, of course, their insurers.

Building back better?

Upbeat projections for the UK construction sector may reflect growing confidence in the economy but, as Deborah Ritchie writes, there is work to be done to repair reputational and risk issues

Construction output was shown in April to have expanded at the sharpest rate for over six years, with robust growth reported across all major categories of construction activity during the month of March, according to IHS Markit and the UK Chartered Institute of Procurement and Supply, as improved demand and contract awards on projects that had been put on hold as a result of the pandemic led to a steep upturn in the sector. Housebuilding was the best performing category, with the fastest growth since July 2020. Strong increases in activity were also seen in commercial construction and civil engineering.

Duncan Brock, group director at CIPS, says the sector was "full of the joys of spring" with a sudden leap into solid growth fuelled by across the board rises in workloads.

"Business confidence was also standing tall with future optimism about the next 12 months the highest since June 2015, which suggests it is mostly plain sailing now that lockdowns are ending and vaccine programmes are underway," he says. "The unfortunate spanner in the works comes in the form of the steepest inflationary rise in raw materials and other construction items since August 2008 at the height of the last commodity price cycle. Supply chains are still under-performing and almost half of the survey respondents said they had experienced longer delays and higher costs. If this continues, it could easily cool the sector down a notch."

Construction companies also reported a sharp increase in purchasing volumes in response to greater workloads. The latest upturn in input buying was the steepest since November 2020.

Higher demand for construction products and materials contributed to longer wait times for deliveries by suppliers. Around 41 per cent of the IHS Markit/CIPS survey panel reported longer delivery times from suppliers in March, while only one per cent saw an improvement. Supply constraints and logistics issues were commonly reported by construction companies, especially for imported items. Imbalanced demand and supply for construction inputs led to the steepest increase in purchasing prices for over 12 years. Survey respondents widely noted that suppliers had cited Brexit and COVID-19 as reasons for price hikes.

Commenting on the supply chain risks, Tim Moore, economics director at IHS Markit, which compiles the data, says: "Constrained supplier capacity and stretched transport availability continued to pose challenges for the construction sector in March. Short supply of products and materials pushed up purchase prices at the fastest rate since August 2008.

"Continued pressures on supply chains are expected in the near-term, but these concerns did little to dampen confidence about the business outlook. The latest survey pointed to the strongest growth projections across the UK construction sector since those reported during a post-election bounce back in June 2015."

The uptick in activity will welcome

news in a sector which has lately been attracting attention for all the wrong reasons – with fire safety issues an ongoing topic of concern across the country.

Numerous issues influencing risk management have already been identified by the Hackitt Inquiry established in the wake of the Grenfell Tower disaster.

A recent industry survey published by the Construction Leadership Council highlighted significant cost increases and the introduction of new restrictions on professional indemnity cover following a period of difficult underwriting conditions and deteriorating claims performance – driven partly by endemic problems within the construction industry itself, according to members of the International Underwriting Association's Construction Professional Lines Working Group.

The IUA is calling for improvements to regulation and culture, prioritising quality construction and safety over cost-cutting. Chris Jones, IUA director of legal and market services, says the construction industry and professional indemnity market have both experienced extremely challenging business conditions.

"Insurers have handled a great many claims arising from fire safety issues and the use of cladding, but although high rise residential buildings are the biggest worry there are also more widespread risk management concerns.

"We are encouraged by a proposed overhaul of the regulatory framework, but it is clear that many historical liabilities have yet to develop into claims and this remains a key factor for insurers in their underwriting assessment.

"A shift in culture is required in order to overcome continuing uncertainty about the enforcement of regulation and a lack of oversight and accountability in the construction process"

"A shift in culture is required in order to overcome continuing uncertainty about the enforcement of regulation and a lack of oversight and accountability in the construction process."

The IUA welcomed many of the recommendations in Judith Hackitt's building regulations and fire safety report. Particularly important, it says, is the creation of a new building regulator to better identify the duties of those involved in the construction process and to ensure more robust oversight throughout the lifecycle of a building. Reform should not, however, be restricted in focus to high-rise residential buildings.

In other insurance-related developments, the Chartered Insurance Institute has been exploring the pros and cons of evergreen policies, which, they argue, could bring more control, improved client relations, better retention rates, and a useful hedging mechanism in what experts believe is a hardening market.

Insurers are not alone in calling for change in the construction sector. A London South Bank University study recently went as far as to say that the recent collapse of Carillion highlights the sector's endemic 'corporate deviance'.

The LSBU study outlines how, following the collapse of a major financial institution like Carillion, individuals and teams in the wider construction sector are prone to explaining away or normalising discrepancies and problems, unintentionally reducing awareness of the potential consequences of that deviant behaviour. This not only stops the company from following codes of practice, but it also prevents it from anticipating and managing reputational issues and structural internal crises, the report warned.

By performing a qualitative analysis on the collapse of the construction giant, the researchers identified the most common deviant practices and sources of 'normalisation of deviance' embedded in the sector. The findings suggest that 'normalisation of deviance' lies not only internally, but also externally, in the wider industry environment in which construction organisations operate.

The report's authors say the results of their study should sound an alarm bell, and are calling for structural reform of the construction industry to prevent the negative effects of corporate deviance.

Dr Sara Hajikazemi, senior lecturer in project management at LSBU's Business School, comments: "Our research shows that 'normalised deviance' has always been present in the construction sector. "What is concerning is that, as happened with Carillion, construction companies currently lack an early warning system that could alert them to emerging signs of deviant corporate behaviour and malpractice. This means that the construction industry is still likely to be at risk of falling prey to 'normalised deviance' and its damaging consequences in future."

The CII's paper can be found at https://www.cii.co.uk/news-insight/insight/articles/evergreen-policies-the-future-of-construction-insurance/98677

Deborah Ritchie is editor of CIR

Tackling modern slavery in construction supply chains

With the tightening of reporting on the horizon, many businesses are turning their attention to how to better mitigate the risk of modern slavery within their operations. Collaboration is key, says Gareth Rondel

The Modern Slavery Act 2015 requires businesses with a turnover of more than £36 million to publish an annual Slavery and Human Trafficking statement. This statement should set out what has been done to identify and eliminate the risk of modern slavery within the business and its activities, including within supply chain relationships. For most organisations this should include an assessment of the material risk posed by modern slavery.

When the Modern Slavery Act was introduced, it was widely regarded as one of the strongest pieces of anti-slavery focused legislation in the world. Around 1,700 businesses fall within its scope, with the intention that it would create a trickle-down effect that would see SMEs tackle modern slavery as a matter of course. In reality, the focus has remained mainly within larger organisations and modern slavery isn't being scrutinised closely enough in many supply chains. In fact, recent research suggests that modern slavery and labour abuses likely exist at some stage within every supply chain, with those who haven't found it yet simply not looking hard enough.

In July 2018 the Home Office commissioned an independent review of the Modern Slavery Act which recommended improving reporting quality and clarifying the scope of reporting organisations. In response, the government has committed to a number of changes. While it is not yet certain when these measures will come into force, commitments include: strengthening section 54 (transparency in supply chains requirements) of the Act, setting a single reporting date for September each year, requiring group statements to name all entities covered by the SHT statement, and obligating companies to specify the date when SHT statements are signed by directors/the board.

It will also become mandatory for SHT statements to cover six topics which are currently optional. The structure of topics may change but they include organisation structure and supply chains; slavery and human trafficking related policies; due diligence processes; risk assessment and management; key performance indicators to measure effectiveness of actions; and training. In addition, the update will likely see public sector bodies with budgets of greater than £36 million expected to comply with the Modern Slavery Act.

Another major development was the launch in March of a central registry for modern slavery statements. Companies of all size are encouraged to lodge a copy of their SHT statement on the registry which can also be used to check what organisations are doing to eliminate modern slavery from their operations and supply chains. Any organisation can add their

SHT statement to the registry, regardless of whether it has been produced as a mandatory requirement or voluntarily.

As expectations around the mitigation of modern slavery grow, so too does pressure on SMEs to show they have a handle on the issue. SMEs make up 99 per cent of private businesses in the UK and employ 17 million people – 13 million of these working in small businesses with fewer than 50 employees. Nearly a fifth of these businesses operate in the construction sector. SMEs are the eyes and ears on the ground and are often well placed to identify modern slavery yet frequently lack the resources to tackle the risk.

The government has emphasised that industry-level collaboration is critical to effectively addressing shared challenges including modern slavery; engaging with supply chains is essential.

CHAS advises creating a policy, publicising it and working with your supply chain to do the same. Your policy should include clear goals and a plan to monitor performance. As a risk manager you will be looking at where the risk is greatest – set an audit regime to sample performance across your supply chain partners, but focusing on those identified as carrying the greatest risk.

Be vigilant and encourage your supply chain to do the same. Make it a prerequisite that partners have their own policy statement and can demonstrate its effectiveness through data, or that they adopt yours if they don't have one in place. Some partner organisations may have policies that go beyond your own – this is a great opportunity to learn from others through engagement and identify which practices you could adopt.

Gareth Rondel is sustainable business lead at CHAS, the Contractors Health and Safety Assessment Scheme


EVERYTHING YOU NEED FOR GRC, FULLY INTEGRATED
From ERM to Business Continuity to Compliance Management, unify the entire GRC process. Turn insight into action and monitor progress.
ORIGAMI RISK
ORIGAMIRISK.COM
© 2021 ORIGAMI RISK

Beyond insurance

If there are solutions to be found to today's risk challenges, they are most likely to be found in the London insurance market, writes Sheila Cameron

The London Market Group and the Boston Consulting Group recently published a report – *Beyond Insurance: A Client View*, in which the opinions of over 40 clients from four major industries - IT, financial services, consumer and retail and energy, were sought to understand the trends disrupting the patterns of risk today.

The objective of the study was to listen to the customers who place business in London. What we heard very consistently is that businesses are increasingly dependent on others for their success. This brings with it risks which are not entirely within businesses' control. It is no longer just about physical assets and services that a company can see, manage and protect. Companies need third party providers to deliver an increasing proportion of their products and services. They rely on AI and new tech to improve them and engage with influencers and social media to market them. These new business models involve a wide range of new risks for which products and services are required to mitigate and manage them.

One of the main trends highlighted by the interviews was the impact of societal change and how those challenges are being accelerated by technological and economic shifts. New communication technologies, for example smartphones, social media, instant messaging and so on, have 'democratised' many of the functions of the media. Globalisation and changes in traditional labour models – such as the gig economy, have occurred at the same time as an apparent acceleration of political unrest and change in many mature economies. Our conversations with London Market clients highlighted two key issues that are shifting the risk landscape for businesses across sectors.

Increasing importance of brand and reputation

Most clients interviewed, across all sectors and geographies, pointed to reputational risk as an emerging key risk on their CRO or CEO agenda; for them, increased adoption of social media and review culture has heightened the risks that reputational incidents pose. As the business risk manager of a global energy company based in Europe put it: "What would have been deemed a normal operational side effect ten years ago is a news headline today."

Moreover, consumers are articulating an increasing concern about the ethical conduct of businesses from which they buy.

"The convergence of mobile and social media is intensifying the impact of reputational risk for organisations and is driving them to fundamentally rethink their approaches to risk management"

Report insights

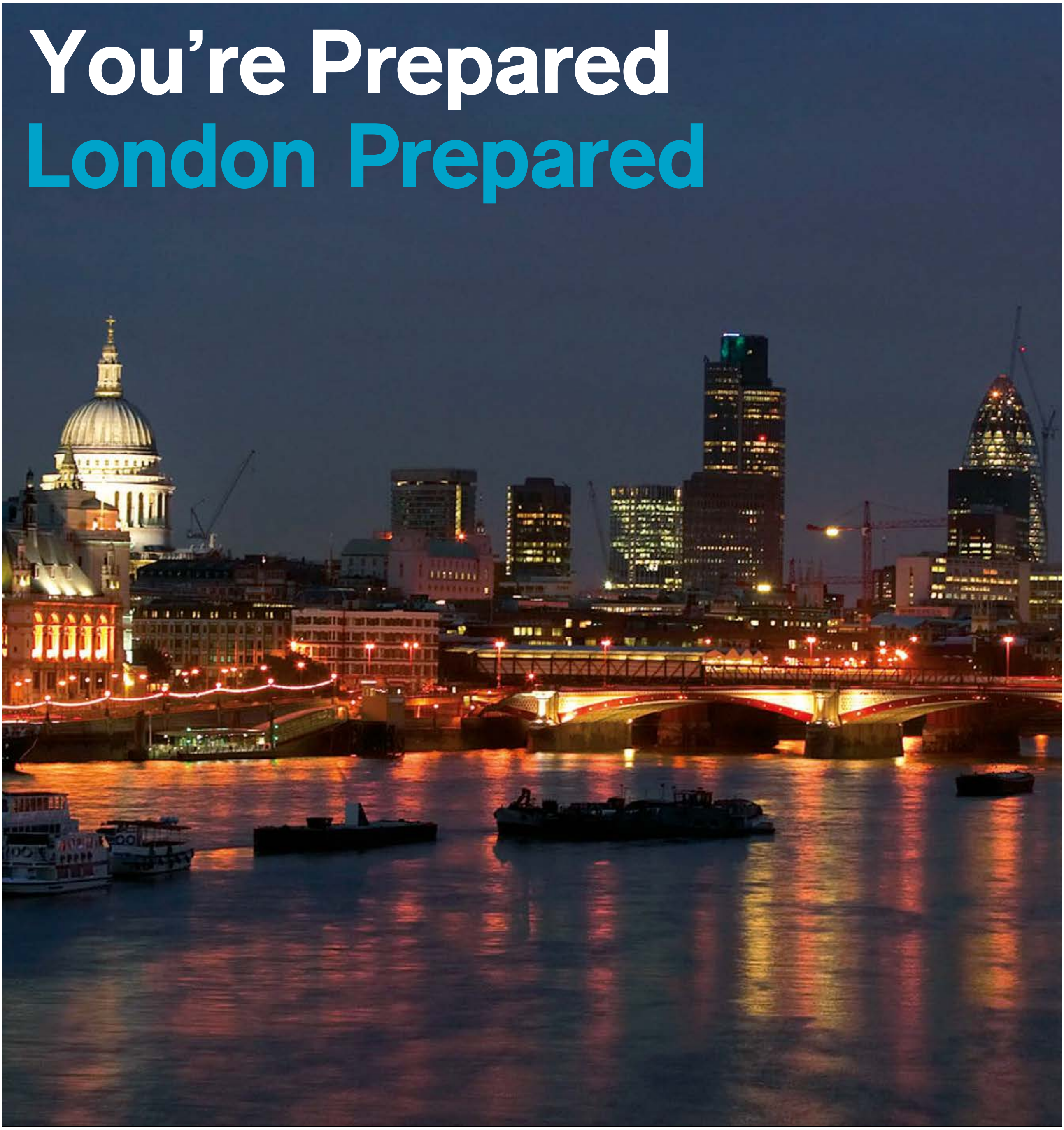
- An estimated US$1.25 trillion was spent on digital transformations globally in 2019, versus a projected US$2.3 trillion by 2023 (IDC)
- Increased automation will allow machines to go from completing 29% of total task hours in businesses in 2018 to completing 52% of total task-hours by 2025 (WEF)
- 60% of business executives in the 20 leading economies have reported that COVID-19 has accelerated their digital transformation plans (IBM Institute for Business Value and Oxford Economics)
- 5G has up to 100x faster data rates and significantly improved bandwidth compared to 4G, enabling broader applications of internet of things, machine learning, artificial intelligence, virtual reality and augmented reality (Thales Group)
- 70% of Chinese consumers use mobile wallets regularly, with e-commerce forecast to account for 12% of the country's GDP by 2022 (Merkator Advisory Group)
- Bank cost savings via chatbots to reach US$7.3 billion by 2023, up from an estimated US$209 million in 2019 (Jupiter Research)
- By 2025, 50% of enterprises are forecast to use AI systems in their operations, up from fewer than 10% in 2020 (Gartner)
- By 2023, 40% of all enterprise workloads (IT applications running the core functions of a business) are forecast to be deployed in cloud platforms, signifying a doubling since 2020 (Gartner)
- Adoption of AR and VR technologies has grown 79% year-on-year since 2016, up from US$6.1B in 2016 to US$18.8B in 2020 (BCG/ Mordor Intelligence)
- The IoT market stood at US$251 billion in 2019 and is projected to reach US$1.5 trillion in 2027, with a 25% CAGR in the forecast period (Fortune Business Insights)

The result is that companies are responding by emphasising their environmental, social and governance credentials, which then puts them at greater risk of reputational damage if they underperform against those targets.

Fossil fuel companies interviewed reported a change in the public response to incidents resulting from their operations. They pointed out that despite diminishing profit margins reputational risks now require ever more investment to deal with operational incidents in an economic environment that is already challenging. "The reputational aspect of social responsibility is skyrocketing," said the head of business risk at a top 10 global energy producer in Europe.

In line with the increasing pressure to protect against reputational damage, clients are struggling to quantify their reputational value and monitor the performance of their reputation and brand. Most clients were not yet aware of existing independent indices to benchmark brand or reputational performance. The convergence of mobile and social media is intensifying the impact of reputational risk for organisations and is driving them to fundamentally rethink their approaches to risk management.

The impact can be three-fold: consumer backlash, shareholder, or investor pressure and/or loss of key employees or business partners, and in many cases companies know they need external help to survive. Several SMEs reported a need for access to external crisis management experts as they do not have those resources in-house. Meanwhile, larger corporates, especially those involved in high-volume low-margin



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

business, highlighted a potential need for cashflow support if a reputational crisis were to trigger a sudden revenue crunch. Larger, publicly-traded companies are becoming more acutely aware of the need for appropriate reputational crisis response when an incident occurs, with new financial contingency planning and crisis management protocols being developed either by in-house teams or selected external partners.

Increased litigation activity

Concerns were raised by almost all interviewees about mounting regulatory, activist and public pressure. Multiple clients highlighted class action cases they were fighting from a range of sources. For instance, a global tech company headquartered in Asia reported an increase in litigation from employees worldwide due to working hours, cultural sensitivities, or mental frustrations coming from remote working. The unpredictability of the origin of litigation was highlighted as another concern which makes it increasingly difficult to protect against. A director of risk management for a national retailer in the US told us: "We recently got sued for a shooting that happened on one of our supermarkets' parking lots. We had nothing to do with it, nothing we could have done. But they sued regardless." Emerging litigation themes mentioned include whether

"What would have been deemed a normal operational side effect ten years ago is a news headline today"

sugar needs to be treated as the 'new tobacco'; concerns about plastic usage in products and packaging; and being held responsible for high carbon emissions as a contributor to climate change.

So, whether it is banks concerned about fake news, tech companies worried about the liabilities for artificial intelligence, start-ups wanting to protect the value of their intellectual property or investors in renewable energy struggling with the increased unpredictability of the weather, none of the challenges identified are easy to address. But clients' needs are clear and the opportunity for London significant.

If there are solutions to be found to these challenges relating to risk, they are most likely to be found in the London insurance market. This is the only place that brings together the breadth of expertise, flexibility of thinking and weight of capital to address the universe of risks that decision makers are facing. This report offers compelling insights for everyone in the market to start conversation with buyers and business partners on how the London Market can continue to serve its clients whatever circumstances they face.

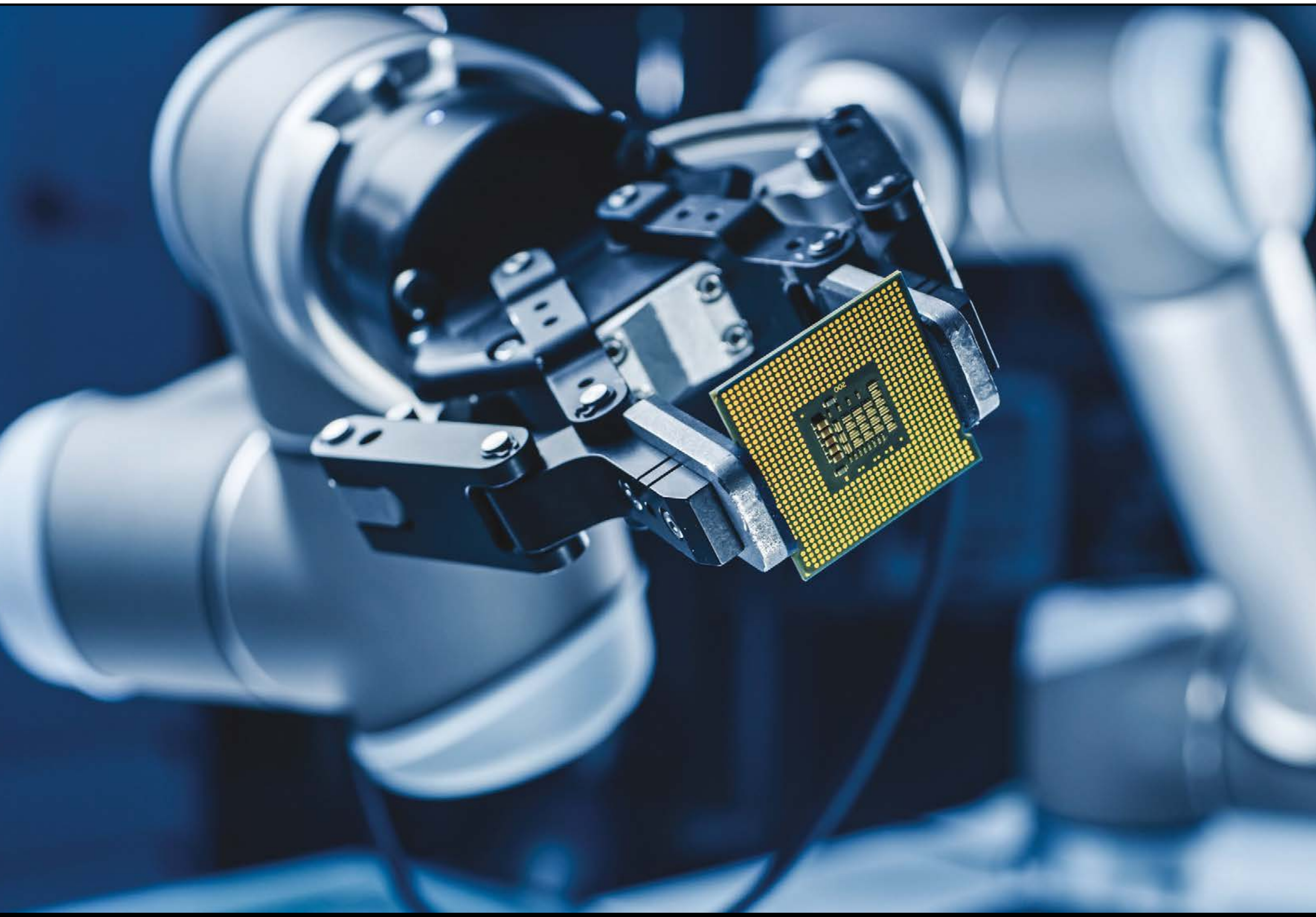
Read the LMG's report in full at visit https://lmg.london/document/beyond-insurance-the-client-view-digital-version/

Sheila Cameron is CEO of the Lloyd's Market Association

Sponsored by

TOKIO MARINE HCC

CIR
CONTINUITY INSURANCE & RISK



Of the many sectors of business, manufacturing companies are among the most at risk from cyber threats. How has the sector evolved to make it so vulnerable and what does the task of managing cyber exposure in a manufacturing company look like? CIR's latest podcast with Tokio Marine HCC sought to answer all these questions and more.

Hyper automated = hyper exposed

Hyper automated = hyper exposed

Managing cyber exposure has become the number one consideration for increasingly connected manufacturing companies. CIR's latest podcast with Tokio Marine HCC discussed the challenges

Why has it become so important to address cyber risks in the sector?

Xavier Marguinaud: Cyber threats are a reality for all companies today, of course, but given the high level of automation in manufacturing, the industry is particularly vulnerable.

Over the years, this industry has experienced some of the most amazing evolutions, even revolutions: from the steam power revolution to the Henry Ford assembly line and the automation era – or Industry 3.0 – to today's Industry 4.0 with its autonomous and cyber physical systems and features. Unfortunately, security around those new and innovative technological elements has never been proactively addressed. It's not unusual for industrials to suffer a cyber incident these days; and they are becoming more difficult and costly to mitigate. According to the 2020 IBM *Cost of a Data Breach* report, the average cost of a data breach in the sector is almost US$5 million. The same report suggests that malicious attacks are responsible for 54 per cent of cyber incidents.

How do you perceive cyber exposure in the industry as a whole?

Florian Sättler: The most frequent attack vectors are remote desktop protocol compromise, usage of software vulnerabilities and e-mail phishing. Attackers will always try to find and exploit those smallest vulnerabilities and weakest links – and, ultimately, human error can never be 100 per cent avoided.

Particular to the manufacturing industry are the interfaces between IT and OT. OT infrastructures tend to be particularly vulnerable since operating systems often cannot be updated and patched appropriately, for example due to warranty and guarantee-related restrictions from suppliers. Companies with different levels of IT integration at different sites and within different networks can also result in large cyber security inconsistencies and therefore increased vulnerabilities.

What are the most common and perhaps the most hidden exposures?

Gülsah Dagdelen: It won't surprise you when I say ransomware attacks are currently the biggest nightmare for most cyber insurers! The impact of such an attack can be massive, as once it infects one production site it can self-replicate to others. Recently, the increase in remote and WFH set-ups has allowed threat actors to leverage new attack vectors. An improperly secured remote desktop protocol continues to be a big vulnerability exploited by these attacks. Once they obtain admin privileges, the company can be fully compromised, leading to data exfiltration and encryption within hours or days. The industrial internet of things is also a fast-growing threat for manufacturing companies.

When it comes to risk management, what are the minimum requirements for your clients?

FS: From an organisational point of view, it's crucial to pay the highest attention to cyber security matters throughout the entire company, up to and including board level. Unfortunately, what we often see is that this prioritisation of cyber security only comes after a severe incident which acts as a wake-up call.

From a technical and operational point of view, the key elements we recognise are once again: security awareness throughout the workforce.

Besides and despite these prevention measures, you will never be able to prevent cyber security incidents fully, but in order to limit their impact, it's important to plan for the worst-case scenario and have sufficient crisis response and business continuity plans in place. The destruction of the IT environment can lead instantly to the inability to manufacture or to trade. As we have repeatedly observed, nothing works without the availability of key IT infrastructure, especially ERP data and warehousing systems.

What key underwriting elements do you take into consideration to assess risk maturity?

GD: The list is quite extensive as you can imagine, but to focus on a few key elements: a consistent approach to cyber security throughout the company and its subsidiaries plays a key role. Then there is strong network segmentation, especially between IT and OT but also between the production site itself. In an ideal version of network segmentation, we would look for subnetworks which would be completely separated – with completely different security and IP zones and connecting at very limited points to avoid lateral movement. The recent SolarWinds and Microsoft Exchange server attacks also proved once again the importance of patching; and the management of privileged accounts is also valuable – no users should be assigned administrative access unless absolutely necessary. Back-ups still remain a key element for us as well. Data should be backed up on a regular basis, for example with a weekly (full) back-up and a daily incremental back-up. Naturally, the integrity of those back-ups should be regularly tested.

When it comes to incidents themselves, are there any particular stories that stand out?

Isaac Guasch: Unfortunately, we have lots of these stories! But two stand out as representative for different reasons. The first relates to motorcycle manufacturer Honda, which suffered a ransomware attack in mid-2020. What makes this attack different from the others is that it was performed by a variant called snake ransomware, also known as EKANS or Snakehorse.

This snake ransomware is written in a specific programming language called Golang containing a type of obfuscation not typically seen in this type of malware. Basically, what the programme does is removes shadow copies and kills the processes related to SCADA and industrial control devices which are the main systems in the OT environment and therefore essential systems in the manufacturing sector. In addition, the malware also kills processes related to machines, remote management tools, network management software and others. After this the software encrypts the files on the devices, but this one skips the Windows system folders and system files which again makes it very difficult to detect. This case shows us that ransomware can be quite tailored to specific industries.

The second story relates to airplane maker Bombardier. In February, data from the company was posted on a ransomware leak site. The company confirmed that the attacker had revealed personal and other confidential information relating to employees, customers and suppliers, as well as some confidential design documents for various airplanes and plane parts. In this case, the forensic analysis concluded that a breach was produced by exploiting a vulnerability affecting a third-party file transfer application.

What are the most relevant response elements in your experience?

FS: Internal processes and diligence are key factors in responding to such an incident. It's hugely important to not only have the IT and IT security personnel but also operational managers and especially the board form an integral part of the crisis team. Firms must also know what expertise they have available in-house and what they need to contract externally. This could be IT forensic and security support or legal advisors.

Quite often – and this is certainly the case with Tokio Marine HCC and Crawford and Company – cyber insurance companies and their partners would even provide such specialist vendors to their policyholders. It is also important to bear in mind that in the event of an incident, there is very likely to be a huge workload on the internal IT staff, so it is likely to be necessary to have extra IT resources available. This will all need to be contractually agreed pre-incident, along with a service level agreement ensuring immediate availability in such an emergency case.

In the case of ransomware in particular, back-ups are extremely important.

What additional trends and developments can you share with us?

IG: I foresee more targeted malware for SCADA industrial and corporate systems. It is difficult to keep pace with these new threats, and even harder to detect them. There will also be a level of diversification on the risk exposure as manufacturing companies will not be only exposed to business interruption but also to data leaks and extortion. The second major trend I see is that of hyper automation using machine learning, artificial intelligence and blockchain technologies. For me, hyper automation equals hyper exposed.

These are just a few highlights from this podcast, which you can listen to in full at cirmagazine.com.

Get in touch with Tokio Marine HCC to discuss cyber exposure in industrial control systems, connected products and the industrial internet of things www.tmhcc.com

Xavier Marguinaud
Head of Cyber
Tokio Marine HCC

Gülsah Dagdelen
Cyber Manager – Continental Europe
Tokio Marine HCC

Isaac Guasch
Cyber Security Specialist
Tokio Marine HCC

Florian Sättler
Engineer & Economist
Technical Expert
Crawford & Company (Deutschland) GmbH

NATIONAL INSURANCE AWARDS 2021

2021 Shortlist

Commercial Lines Broker of the Year

- Addingstone Insurance
- Business Choice Direct
- McCarron Coates

Claims Team of the Year

- Addingstone Insurance
- Brit Insurance
- FMG
- Markel UK
- Nexus Claims

Commercial Lines Specialist Broker of the Year

- Coleman Marine Insurance
- McCarron Coates
- Stride Underwriting

Personal Lines Broker of the Year

- P J Hayman & Company
- Vizion Insurance Brokers

Travel Insurance Award

- Allianz Partners Insurance
- battleface
- Goodtogoinsurance.com
- Voyager Insurance Services

Claims Initiative of the Year

- Brit Insurance
- Charles Taylor
- Direct Commercial
- Direct Line Group
- Gallagher Bassett
- Markel UK
- Zurich Insurance & Carpe Data

Lloyds and the London Market Award

- Direct Insurance London Market
- Kovrr
- Munich Re Syndicate

Cyber Product of the Year

- FM Global
- Kovrr
- QOMPLX:UNDERWRITING

InsurTech Award

- Adapt Ready
- Autonomise.ai by VisionTrack
- DAC Beachcroft in collaboration with Automated Insurance Solutions
- DriveXpert, Privilege Insurance (Direct Line Group)
- MS&AD TX Connected
- RightIndem
- RMworks by Griffiths & Armour
- Tempcover

Commercial Lines Insurer of the Year

Special category – To be announced on the night.

Communications Team of the Year

- AXIS Capital
- Bupa
- Direct Insurance Group
- Paymentshield

Innovative Product Award

- Kingsbridge
- MS&AD TX Connected
- QOMPLX:UNDERWRITING
- Tempcover
- Willis Towers Watson

NATIONAL INSURANCE AWARDS 2021

2021 Shortlist

Innovative Product Award - Technology

- Adapt Ready
- Cazana
- Kovrr
- RightIndem
- RMworks by Griffiths & Armour

Initiative of the Year

- InfraGenie by Mphasis
- Kovrr
- RMworks by Griffiths & Armour
- Sedgwick
- Willis Towers Watson (A Willis Re, Climate and Resilience Hub and Alternative Risk Transfer Collaboration)

ESG Award

- Sedgwick
- Willis Towers Watson (A Willis Re, Climate and Resilience Hub and Alternative Risk Transfer Collaboration)

Specialist Coverage Award

- Coverdrone
- Medicash
- Paymentshield
- Tempcover

Growth Company of the Year

- Arch Insurance
- Lloyd & Whyte
- Nexus Underwriting
- Rokstone Underwriting
- Travelers Legal

Insurance Recruiter of the Year

- Boxtree Recruitment
- Idex Consulting
- Insure Recruitment
- Lawes Consulting Group

Insurance Law Firm of the Year

- DAC Beachcroft
- Travelers Legal

Digital Insurance Award

- Bupa
- Direct Line Group - Green Flag
- Ki Insurance
- RMworks by Griffiths & Armour
- Tempcover

Inclusion and Diversity Award

- Bupa
- Inclusion@Lloyd's Partner Networks
- Insurance Cultural Awareness Network

Loss Adjusting Award

Special category – To be announced on the night.

Brought to you by Insurance Today

In partnership with CIR Continuity Insurance & Risk

Supported by Chartered Insurance Institute

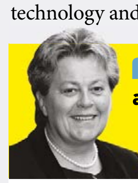
Industry views

There are some truths we ought to take as self-evident in modern risk management. Firstly, we know that good risk management makes good business sense; secondly, we know that we live in a world of high velocity change and complexity; and thirdly, we know that the world has changed for ever.

In recognition of this context, risks shouldn't be managed in artificial silos; risks with high impact low probability profiles can emerge at speed with devastating effect; and risks are increasingly assessed in a world of intangible assets.

In this new environment, we need to step up together to drive change. We need to resist passivity and COVID inertia in order to seize the opportunities, particularly by continuing to break down siloes, so that the functions of risk management, insurance, business continuity and crisis management work together seamlessly as effective pillars of managing risk and building resilience. Our risk transfer partners increasingly realise the world is changing. For them the model is changing, too, but further change is needed to stay relevant. The insurance market is going from a passive risk financing posture to a focus on more active risk management. Risk financing is no longer enough, particularly given the shift in emphasis from physical bricks and mortar assets towards intangible risks that increasingly dominate the business landscape. With the changed emphasis, risk takes the lead, requiring insurance and enterprise-wide risk management to work side by side to avoid siloed thinking. Artificial barriers can exist between traditional product types and underwriting lines and classes. To be blunt, is the tail wagging the dog? The future should be a more responsive insurance market, with an increasingly risk-based pricing approach, which ensures the efficient deployment of capital and strives for a proactive reduction in extreme risk event losses, rather than a reaction to post-event losses.

We should never let a crisis go to waste. 2021 provides a great opportunity to seize the lessons that commonly emerge in moments of disaster. We need a shared purpose and challenge the synergy between risk and insurance, harnessing change, technology and stakeholder engagement to flourish together.



Julia Graham is deputy CEO and technical director of Airmic

In association with airmic

Nearly 19,000 vessels passed through the Suez Canal last year, carrying around 12% of global trade. Therefore, the closure of the canal for six days in March during the stranding of the ULCV Ever Given was a global news story from the start. But over a month later, the insurance consequences of this story are only just beginning to become visible.

The Ever Given itself has been detained in Egypt pending settlement of a US$1bn claim for compensation made by the Suez Canal Authority. But for supply chain managers and their insurers everywhere, in the long-term, this incident may come to be remembered for something other than its impact on the marine market. Much more significantly, it seems that for many, the impact of coronavirus on stocking and shopping habits, followed by the Suez Canal closure, has been a trigger for the rethinking of supply chain planning and inventory control. The impact has been especially marked in a year when pressure around climate change became markedly higher. According to Dun & Bradstreet, procurement managers are highly concerned about ESG issues, and their influence on supply chain planning.

Last month global shipping giant Maersk's chief executive told investors that the disruption from the Suez closure would cause companies to move away from just-in-time supply chains and towards keeping much higher inventory levels; a tectonic shift which will impact insurers hugely. Firstly, the impact will be felt in terms of values as stock in warehouses surges, and corporate risk shifts towards inventory and storage instead of just-in-time and transport risks. Secondly, the lever that many firms will use to tighten their supply chain planning will be technology. With an amazing 98% of procurement professionals struggling with supplier data management, cyber risks must also be considered a growing risk.

For insurers, the lesson is clear. Use the supply chain shocks of 2021 as a trigger to review exposures. For risk managers, the call to action is also loud. While change may be traumatic for all, perhaps the outcome of this year of change will be a more resilient supply chain, and one where risks are better identified, and perhaps even better insured.

Jim Sherwood is a partner at BLM and chairman of Global Insurance Law Connect

In association with GLOBAL INSURANCE LAW CONNECT

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

COVID-19 has shown the importance of running effective, efficient and flexible business operations and risk management practices. Whilst the pandemic is sadly not over and increasingly rife in countries such as Brazil and India, valuable lessons have and are being learned.

Building good risk management into everything you do should be paramount. Don't see risk as something that sits elsewhere in the organisation, perhaps in a team labelled 'risk management'. At work, I expect all my colleagues to talk about the risks in whatever they do, whether it is developing strategy, thinking about an acquisition, looking at building the talent in our organisation or going about their day-to-day jobs.

It is impossible to prepare for every eventuality and very few organisations will have been prepared specifically for COVID. However, organisations can prepare for business disruption and set up structures such as incident management teams that allow them to react quickly to unfolding events. Investing in data sources to keep abreast of changing circumstances is also an important part of risk management. Investing in ensuring you have a culture within your organisation which means you are aware of and discuss risks that face you, you plan appropriate mitigation, you set indicators so you can see risks unfolding and you are ready to react should things go wrong: these are all worthwhile investments which don't require you to plan for every specific risk that may impact you.

In a survey carried out by the Institute early in the crisis, we found that 32% of organisations surveyed had not considered pandemic risk or anything similar before it happened. Of those organisations, the same percentage had not planned what to do should that hit. One fifth of organisations who considered pandemic risk didn't then do anything about it.

I think that, as lessons are learned, we will find that the organisations that coped best with the crisis were those which were able to react quickly to unfolding uncertain circumstances and I think there will be a high correlation between those organisations and those that had prepared for similar eventualities. Wargaming unrelated scenarios can help get an organisation's DNA to a place where it improves its capability to respond to unforeseen events.

We mustn't allow the magnitude of the current crisis to obscure the other major (and interconnected) risks that we all face. We still need to tackle climate change, cyber risk, supply chain disruption, economic and geopolitical volatility, to mention just a few. The IRM, the IOR and our wider global risk management community stand ready and confident to lead the response.

My advice to anyone thinking of a career in risk or developing their staff is that there is huge value in studying the subject. Having a solid grounding in the principles and practices of risk management will pay dividends in helping your organisation understand and manage its risks. I would also say that change is a constant, so build personal resilience to deal with and, if possible, lead that change. Finally, build your own networks. This will help you navigate change and be effective in work but it will also help combat any feelings of isolation you may have during difficult, turbulent times.

Good risk management is a competitive advantage for organisations but also for individuals and there's never been a better time for organisations to invest in their staff. The IRM's enrolment period for our December exams closes on the 31st May. All our qualifications are available via online supported distance learning and are relevant to any organisation, in any sector globally.

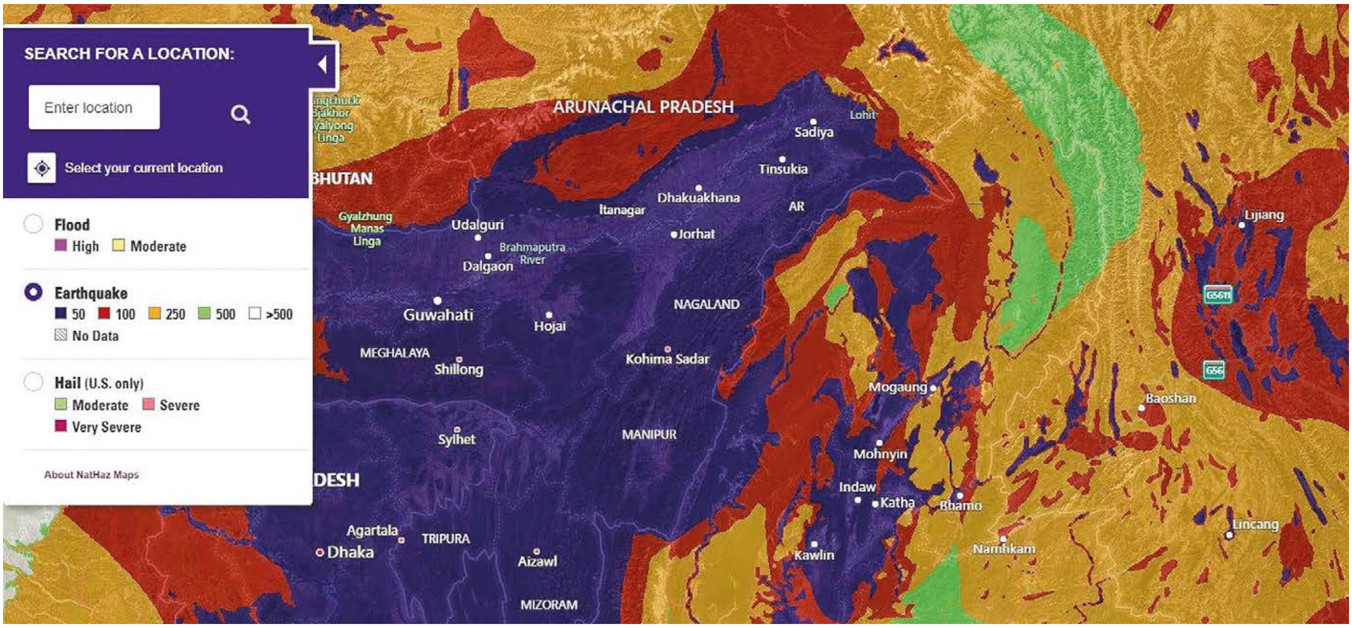
Iain Wright is chairman of the Institute of Risk Management

In association with

irm

Assessing the ever-present risk of earthquakes

FM Global's newest worldwide map presents a complete picture of the risks posed by earthquakes across the globe



Earthquakes cause on average some £29 billion in direct economic loss every year, as a result of destroyed buildings, disrupted supply chains and business interruption.

To address the risk, and to help businesses improve the resilience of their global supply chains, FM Global has compiled what it believes is the world's most comprehensive global earthquake risk map.

Online and interactive, the FM Global Worldwide Earthquake Map is a layer in the company's natural hazards map, which also displays climate risks such as flood and hail. Regions fall into zones based on the return periods of damaging ground motion: every 50 years, 100 years, 250 years, 500 years and 500 years plus.

"The majority of global businesses have locations, suppliers, or customers in earthquake zones but lack a complete picture of the risk," said Brion Callori, senior vice-president and manager, engineering and research at FM Global. "To business leaders, the seismology of an earthquake is less salient than the property damage and business disruption that can result. Our clients' business resilience is the focus of this map."

According to the new map, some regions of the world will see above-average movement to higher risk zones, including the Netherlands, France, Switzerland, Italy, Israel, China, New Zealand, India, Mexico, and the states of California, Idaho, Nevada, New Mexico and Utah. Areas seeing above-average movement to lower risk zones include Spain, Germany, Austria, Hungary, the United Arab Emirates, Thailand, Malaysia, Singapore, Australia, Ottawa-Montreal and the states of Oregon and Washington, and the New Madrid Seismic Zone region.

Free to use, the new map incorporates soil effects and building structural performance to map the return times of ground motions that will damage weak buildings. Integrated soil data also helps determine shaking levels at a resolution of one square kilometre or less. The map also integrates refined thresholds for structural vulnerability to account for varying building quality and contents around the world.

The FM Global Worldwide Earthquake Map employs data and seismic hazard models resulting from their longstanding partnership with the Global Earthquake Model Foundation, a non-profit, public-private partnership that drives a global collaborative effort to develop scientific and high-quality resources for transparent assessment of earthquake risk. In China, a hazard model jointly developed by FM Global and the China Earthquake Administration is used, and in the US, a new hazard model by the US Geological Survey is used.

View the FM Global Worldwide Earthquake Map online at www.fmglobal.com/nathaz

Deborah Ritchie is editor of CIR Magazine

BUSINESS CONTINUITY SOFTWARE

Daisy House, No 2 Golden Square,
220 Chester Street, Aston,
Birmingham, B6 4AH

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

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

RecoveryPlanner
101 Merritt Boulevard, Trumbull, CT
06611 USA and Dartford Kent, UK

Contact Name: Jeff Goldstein, Sales Director

Tel: +1 (203) 455-9990
jgoldstein@recoveryplanner.com
www.recoveryplanner.com
Linkedin: www.linkedin.com/company/recoveryplanner.com/
Twitter: @RP_BCM

Resiliency Solutions Since 1999

RPX BCM Software
Depth, Flexibility & Scope for a Planner, Simple Enough for the Casual User
RecoveryPlanner's all-in-one **RPX** software brings together compliance, resiliency, operational risk and continuity to deliver a mature, integrated solution.

Key Features:
- One Complete Mature Software
- Cloud-based, Strong Security
- SaaS or On-premise License
- Unlimited, Concurrent Licensing
- Multi-lingual UI & Support
- Support in all Time Zones
- Native App - iOS & Android
- Rapid Implementation
- Customizable & Flexible
- Crisis Communications
- Leader in all Gartner's MQ's for BCMP Software

Continuity Consulting
Also available are integrated consulting services to help develop effective Plans and Programs that are tailored to each organization's culture, structure and maturity. Direct representation, support and professional services are available throughout Europe, EMEA and APAC.

Contact us today to see what RPX can do for you!

BUSINESS CONTINUITY, DISASTER RECOVERY & ALWAYS ON INFRASTRUCTURE

Daisy House, No 2 Golden Square,
220 Chester Street, Aston,
Birmingham, B6 4AH

For more information:
Call +44 (0) 344 863 3000
Email Enquiry.dcs@dcs.tech
https://dcs.tech/business-continuity/

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
The Globe Centre, St James Square,
Accrington, Lancashire BB4 0RE

Contact: Ashley Seed

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

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

RISK MANAGEMENT SOFTWARE SOLUTIONS

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

JCAD provides easy to implement and highly effective software for streamlining risk management and claims handling processes in the public and commercial sectors. As a family owned business, we strive to provide excellent, friendly customer support. Our specialist team works continuously to update and improve our products, ensuring our solutions help clients improve efficiency, increase accuracy and save money.

ORIGAMI RISK

Origami Risk
222 North LaSalle Street
Suite 2125 Chicago, IL 60601

Tel: 312.702.5395
info@origamirisk.com
www.origamirisk.com
YouTube: https://www.youtube.com/channel/UCUSGoJ_XoT0nz_K9HJXk2rQ
LinkedIn: https://www.linkedin.com/company/origami-risk/
Twitter: https://twitter.com/origamirisk

Origami is a leading provider of integrated SaaS solutions for the risk, insurance and compliance industry—from insured corporate and public entities to brokers and risk consultants, insurers, TPAs, and risk pools. Our solutions for RMIS, GRC, EH&S, Core Policy and Claims, and Healthcare Risk Management are highly configurable and completely scalable. Origami delivers a full suite of solutions from a single, secure, cloud-based platform accessible via web browser. Our software is supported by an experienced service team who possess a balance of industry knowledge and technological expertise. With our unique service model and highly configurable solution, our expert team implements and provides ongoing support to align with clients' strategic organizational priorities. Since all components are contained within a single, true SaaS platform, scalability is seamless, enabling clients to focus on their priorities while providing access to the latest technology.

PROTECHT
Redefining Risk

1st Floor, 60 Gresham Street
London EC2V 7BB
United Kingdom

Contact: Keith Davies -
Director Sales and Operations,
U.K. & Europe

Tel: +44 (0) 7828 163 802
keith.davies@protechtgroup.com
www.protechtgroup.com
LinkedIn: au.linkedin.com/company/protecht-advisory-pty-ltd
Twitter: twitter.com/Protecht_Risk
You Tube: www.youtube.com/user/ProtechtPtyLtd

The Protecht Group
Protecht helps organisations through deep understanding, monitoring and management of risk. We provide the complete risk solution—comprised of world-class enterprise risk management, compliance, training and advisory services—to government organisations, key regulators and businesses of all sizes across the world.

With 20+ years at the forefront of risk and compliance solutions, millions of incidents managed across thousands of individual risks, and over 25 thousand people attending our training courses to date, we're one of the most respected and influential voices in risk.

Dynamically manage all your risks in a single platform: Risks, Compliance, Health and Safety, Internal Audit, Incidents, KRIs, BCP, and more.

We're with our clients for their full risk journey. Let's transform the way you understand and manage your risk to create exciting opportunities for growth.

RISK MANAGEMENT SOFTWARE SOLUTIONS

riskHive
Software Solutions

riskHive Software Solutions Ltd
Dilkush
Farlers End
Bristol
BS48 4PG

Rebecca.cope-lewis@riskhive.com
+44 7539 592 727

Sandu.hellings@riskhive.com
+44 7768 866 158
www.riskhive.com
Linkedin: www.linkedin.com/company/riskhive/

For over 20 years riskHive have delivered innovative software solutions supported by Subject Matter Experts.

riskHive Enterprise Risk Manager®
is a secure private-cloud risk database that supports your risk management needs as they evolve. Fully configurable to meet the changing requirements of your risk management journey, riskHive ERM supports the way you want to work.
www.riskhive.com

riskHive Arrisca Risk Analyser
is a stress-testing and risk analysis tool that helps you understand, evaluate and assure any Excel spreadsheet. With just a few clicks you can improve confidence in your base spreadsheet models and run Monte Carlo to underpin your decisions.
www.riskhive.com

riskHive's independent Cost Analysis Service (iCAS) has been developed over a 20-year period with UK MoD & industry to deliver fast, high-quality assurance and optimisation of cost, schedule and performance models using proven riskHive tools and techniques.
www.grey-beards.com

Experience. Knowledge. Capability. Expertise.

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

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

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

Our services span:

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

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