Focus Feature
With QBE European Operations

Book review
This month, we read *Futureproof*

Nat cats
Counting the cost of the bushfires

cirmagazine.com

April 2020

CIR

CONTINUITY INSURANCE & RISK

Weinstein and the workplace *Compliance, risk and HR professionals should heed the warning signs*

Eastern horizons *The Middle East remains a crucial business region, but one where balancing risk and opportunity is vital*

Adjusting course *Interconnectivity brings a heightened risk of cyber attack or systems failure for the maritime sector*

COVID-19

From chaos to continuity

View: "There is much debate about the extent to which we have entered a true hard market"

CIR

BUSINESS CONTINUITY AWARDS 2020

NEW DATE

9 DECEMBER 2020

The pinnacle of achievement in
business continuity, security and resilience

London Marriott Hotel, Grosvenor Square

Sponsored by

daisy.

Regus workplace recovery

THE RETAILERS BUSINESS CONTINUITY ASSOCIATION
"Together we Plan, Prepare and Share"

In association with

CITY OF LONDON

Supported by

airmic

ALARM embrace risk

Insurance Today

cirmagazine.com/businesscontinuityawards

Comment

Chaotic scenes in supermarkets, tension and even brawls on public transport over mask-wearing and coughing, fake news, fake remedies, and alarming headlines around the stockpiling and resale of PPE at exorbitant prices all characterise the darker side of what can happen when people are faced with a pandemic.

These headlines were counterbalanced with news of powerful acts of generosity, solidarity and commitment by companies and individuals to pursue the greater good – from restaurants making and delivering free food for frontline staff, entire production lines switching from making their usual products to manufacturing masks and other protective equipment, to shop workers putting themselves in danger to feed locals, and communities coming together to reach out and look after those in need.

Weeks later, and the focus has shifted to when lockdown may end. Already there are signs that it is working in the UK, with the virus' peak expected in the coming weeks. But it is not over yet, and until it is, the focus remains on getting organisations through the crisis.

Some excellent examples of these efforts have been compiled in one of the first reports on the business response to the crisis. Researched by global management consultancy, Arthur D. Little, the report details the actions and reactions among global CEOs in the telecoms, transport and utility industries delivering critical infrastructure services in Asia and Italy during the early spread of the virus, and is recommended reading for risk professionals leading or involved in any element of their companies' own response.

The insights are from leaders who maintained effective operations through the worst of the pandemic and are now preparing to rebuild. The first area of focus was found to be the need to move fast, assume the worst, be comprehensive, and secure employee safety first and operational continuity next. The second focuses on accepting that you may spend "most of your time" on employee communications – keeping up positivity and morale, and, importantly, listening as well as talking. A common theme throughout the crisis has been the value of separate A and B teams for critical operations, support suppliers and ecosystem partners. The ADL report goes further, urging innovation in cash management, and collaboration with authorities and communities.

The final key insight was to start realistically planning for recovery now, despite the difficulties of maintaining a positive attitude in the depths of a crisis. "All the business leaders emphasised the importance of positivity, in terms of both maintaining morale and ensuring the best – and fastest – recovery possible following the crisis," the report reads. "This does not mean false optimism and denying realities, but rather, acknowledging that although the crisis may not be over quickly, it will not last forever. In practical terms, our leaders acknowledged that in the early stages of the crisis, and especially if companies were damaged and focusing on survival, there might be little enthusiasm for working on recovery. Setting up separate teams to focus on this is one way to make progress."

The respondents to ADL's research also recognised that the post-crisis business environment would present a raft of new opportunities. Among them were the creation of efficiencies, increased productivity, and further 'smart working' practices; greater automation and more flexible working; step changes in customer adoption of online services, including potential for new remote products and services, such as diagnostics and testing; and M&A opportunities arising from shake-out and consolidation.

Deborah Ritchie

CIR | Risk Management AWARDS 2020

SAVE THE DATE
11TH NOVEMBER 2020

The 11th annual Risk Management Awards

The pinnacle of achievement in risk management

cirmagazine.com/riskmanagementawards

Sponsored by

Regus workplace recovery

Headline Partner

irm
Developing risk professionals

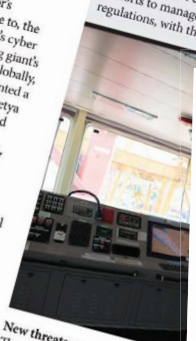
Supported by

airmic

ALARM embrace risk

London Marriott Hotel, Grosvenor Square

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

Contributors
Martin Allen-Smith
Andrew Beckett
Dr Matthew Connell
Ant Gould
Edward Henry QC
Jeremy Hughes
Andy Kane
John Ludlow
Deborah O'Riordan
Iain Wright

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 Wall
London, EC2M 5PD
UK

Tel: +44 (0)20 7562 2400

ISSN 1479-862X
cirmagazine.com

Environmental claims management: pre and post-loss

Response Investigation Remediation

0800 592 827
adlerandallan.co.uk

Adler & Allan
ENVIRONMENTAL RISK REDUCTION

Art of distraction

As expected, the frequency of attempted cyber attacks has shot up amid the COVID-19 outbreak. Andrew Beckett outlines some important considerations for cyber resilience throughout the pandemic, and indeed beyond

In what has felt like a sprint start to a marathon, keeping up with the coronavirus pandemic is leaving businesses with little time to calculate approaches as they are forced to react to daily developments 'on the job'. Unfortunately, in moments of crisis, cyber criminals are known to capitalise on the confusion and, with the peak of crisis not yet upon us, businesses who are aware of the threats to their IT infrastructure will be best placed to mitigate such risks.

Here's what firms should be doing to maintain cyber resilience now and avoid critical moments:

Remote access

The government's advice to avoid 'non-essential contact' means that organisations have and should be implementing work from home policies where it is possible to do so. While this eventuality has looked likely for a couple of weeks, many businesses have not yet prepared their networks with appropriate security and privacy controls to withstand the increased risks this brings. For all businesses, security must be at the top of the list of concerns. Key areas of focus should be:

- Establishing a unified network Connecting to the company network through a virtual private network is important. Unlike disparate networks, which have the potential for many entry points, a unified network offers the greatest protection. Technology teams should be aware of connectivity issues and must ensure systems facilitate simultaneous connections.
- Functionality Can your team carry out their functions as normal? From setting up a phone system to connect everyone, to having access to all the necessary data, it's important for businesses to test jobs from minor to major outside the office.
- Protecting private material Employees may need to print out and safeguard sensitive material. The resolution for this is simple; a cross-cut shredder or a box to store the material until it can be brought in for proper disposal will be effective.

Testing

With events unfolding quickly, actions must follow suit. Testing solutions immediately, under real world conditions, will expose weak spots and enable businesses to efficiently scale up. Organisations must also consider cyber security compromises. Key considerations include:

- Phishing attacks Links sent to employees with compelling subject lines – perhaps playing into people's fears – may result in the downloading of malicious malware gaining access to a firm's network, if clicked through. It is vital that the workforce must be made aware of this type of attack – awareness is key to mitigating this risk.
- Operating security operations remotely What if access to a security operations centre is restricted? Assuming all incidents will have to be dealt with remotely is important, and businesses who can, should simulate running the SOC with remote personnel.
- Third-parties' capabilities Whether an outsourced security provider has your full trust or not, it is worth asking exactly what processes they have in place to manage the crisis. They may never have dealt with one before, so you are within your rights to question the systems and policies in place to ensure that their business is minimising all risks.
- Offline back-ups With ransomware increasing in sophistication and reach, it's vital that offline backups are tested and protected. Experiencing a cyber security crisis during a much broader crisis like this, is potentially catastrophic.

Third-party preparation

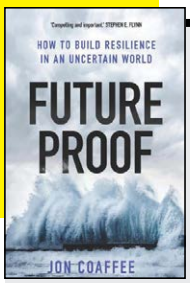
Finally, it's easy to overlook a partner's preparations while getting your own ready, but closing your eyes and hoping they're ready should be the last thing you do. Without a key supplier, operations could halt during a period that will be challenging even for the best prepared. It's vital to communicate throughout the entire supply chain the importance of data and cyber security. Actions should be shared, security discussed and strategic 'what ifs' brainstormed to ensure everyone is taking action.

"Without a key supplier, operations could halt during a period that will be challenging even for the best prepared"

Today's crisis conditions are unpredictable, and the only way to develop resilience to what might lie ahead is to take time to plan systematically. Those who have tested scenarios while building the flexible infrastructure to match, will be best placed to deal with whatever lies around the corner.

Andrew Beckett is managing director at Kroll, a division of Duff & Phelps

Inspiration for resilience professionals



Futureproof: How to Build Resilience in an Uncertain World

By Jon Coaffee, Yale, 2019
Reviewed by Deborah Ritchie, group editor, CIR
yalebooks.co.uk

Every day is a good day to talk about preparing for the future. But yesterday is always the best time to start.

To suggest that the idea of forward planning is new would be ridiculous – especially to the resilience community. But that's not the premise of this book.

Whilst its introduction provides a potted history of risk, uncertainty and society's way of dealing with them throughout the ages and across geographies and cultures (including the obligatory Lloyd's Coffee House story; what book on risk is complete without it?), author Coaffee uses it to set out his stall early on.

To understand fully where the author is taking us, one has first to take a look at where he has come from. Jon Coaffee is Professor in Urban Geography at Warwick University in the UK's Midlands. The focus of his work is on the interplay of physical and socio-political aspects of urban resilience, a topic to which he is clearly deeply committed and on which he has been widely published – with a particular emphasis on the impact of terrorism and other security concerns on the functioning of urban areas. Also relevant to the thrust of this book is his position as co-lead of the University's Global Research Priority in Sustainable Cities.

So, Coaffee's areas of focus, study and interest are specifically urban security, the politics and practices of resilience, counter-terrorism, political geography and disaster management. That is, physical disasters such as those borne out of natural or man made catastrophes – from hurricanes to terrorism. And it is specifically these topics that he explores in *Futureproof*.

In seeking to mitigate risk, the author posits that the traditional approach of planning for specific, known disruptions should be reinforced by anticipating unknown future challenges, and by developing the capacity to adapt to entirely new threats. This, he says, would enhance our ability to bounce back (using our tried and tested traditional methods), and give us a further ability to 'bounce forward'.

"Coaffee believes we now stand at edge of an age of permanent adaptation – with 'new normal' levels of uncertainty and volatility"

That's the 'what', so what of the 'how'? In its nine chapters, one is dedicated to the topic of organisational agility, which looks at such notable developments across the resilience spectrum as the emergence of the doctrine of UK resilience as a response to the fear of terrorism post-9/11, and the appearance around five years later of the notion that resilience might even bring about competitive advantage.This all seems like a long time ago, and indeed the message has permeated far and wide since then.

Just as well, as fast-forward 15 years, and Coaffee believes we now stand at edge of an age of permanent adaptation – one where 'new normal' levels of uncertainty and volatility will compel us to become better able to adapt "in order to cope when everything around us is in flux and find new pathways to navigate our deeply changeable world".

It's at once exciting, terrifying, reassuring and nerve-wracking.

What you won't find in this book is anything on the topic of pandemic planning. Which might be a relief to some readers – not just because we can't go anywhere without reading about COVID-19 (can't go anywhere full stop?), but also because 'other' risks don't cease to exist just because the 'big one' is dominating the front page. Every day.

This not the only book going by this title; there are lots of others – in fact a handful were published in 2019 alone. One in particular, *Futureproof! 13 Things Your Parents Can't Tell You About Tomorrow*, struck me as worth a look for readers with inquisitive teens. Now is as good a time as any to get children acquainted with the concepts of risk and resilience, and how they affect lives and livelihoods today and tomorrow. (You'll have to tell them the Coffee House story yourself, though, as it skips that part.)

News briefing

A round-up of the latest industry news

The Financial Conduct Authority said it expects all firms to have contingency plans in place to deal with the COVID-19 outbreak, as it would any major event, and, along with the Bank of England and the Treasury, was working with a number of firms to assess operational risks and business continuity measures.

> The oil, mining, metals and extractive industries continue to make up the most significant proportion of demand for specialist credit and political risk insurance coverage. So said BPL Global's annual Market Insight report, which pointed to an increase in enquiries from OECD countries – a continuing development from historical demand for CPRI to cover emerging market risk.

The City watchdog later told regulated firms that their designated Senior Manager or equivalent person is responsible for identifying which of their employees are unable to perform their jobs from home, and have to travel to the office or business continuity site.

As more and more businesses implemented remote working practices amid the outbreak, BSI's Cyber Security and Information Resilience team put together a series of tips for businesses and workers as to how to best prepare for working away from their offices efficiently and securely – from protecting confidential business information to effective working patterns and environments.

The Association of British Insurers warned that most businesses will not be covered for coronavirus. In a statement the trade body said: "Irrespective of whether or not the government orders closure of a business, the vast majority of firms won't have purchased cover that will enable them to claim on their insurance to compensate for their business being closed by the coronavirus.

Willis Towers Watson launched a tool that provides real-time information on confirmed global COVID-19 cases alongside clients' property total insured values by location. Part of its Global Peril Diagnostic modelling tool, the new feature will help clients more easily track developments of the pandemic alongside their property assets.

This month, the broker also launched a community group aimed at providing data, knowledge and solutions to its business aviation clients. The group, A Class, focuses on data analytics and risk strategy, equipping business aviation operators with data and expertise to help them analyse and mitigate risks.

A report published by the British Standards Institution highlighted the ongoing risks relating to the coronavirus outbreak, widespread protests and climate change as key drivers of global supply chain disruption. Using data from its SCREEN tool, BSI predicts these trends will dominate the global supply chain throughout the year ahead.

Supermarkets emerged victorious in the crisis communications race, despite facing huge challenges with supply chains and delivery services amid the coronavirus pandemic, including empty shelves and suspended online shopping operations due to extreme surge in demand amid the coronavirus outbreak.

The British Insurance Brokers' Association welcomed the new chancellor, Rishi Sunak's approach to Insurance Premium Tax. Not changing the current rate, which is already at a significant 12 pence in the pound of every premium paid, will help businesses and consumers to afford the insurance protection they need, it said.

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

The number of digital accessibility lawsuits filed in the US between 2017 and 2018 was found to have increased by 183%. In one of the more high-profile cases, Domino's Pizza was found guilty of not making its website app accessible for use by people with visual impairments, and was forced to make adjustments to improve user experience.

A week after Windstorm Ciara, Windstorm Dennis brought flood- and wind-related damage across parts of Europe, with Germany, France, Belgium and the UK bearing much of the brunt, and killing at least six people. Total economic losses from these events are expected to exceed £78m, and ongoing flooding continues to effect transport infrastructure.

Poor employee health has overtaken IT and telecoms outages to become the most frequent cause of disruption to businesses globally, according to the latest global survey of 665 businesses by the British Standards Institution and the Business Continuity Institute in their ninth annual Horizon Scan Report.

Commercial property insurance policies are leaving businesses exposed to technology risks such as data loss, according to Mactavish, which reported a significant increase in policies that have removed this element of cover, even if the loss arises from a 'traditional' property loss, such as fire.

Regulatory activity under the European Union's General Data Protection Regulation increased during 2019, but not quite to the 'mega-fine' degree that had previously been feared. The most notable outcome from a year with the GDPR was instead the considerable variance in penalties issued by different regulators throughout the bloc.

Negligent data management at Virgin Media exposed the personal details of 900,000 of its customers, after a database was left unsecured for ten months, and during which period was accessible online. Partner at city law firm DMH Stallard, Jonathan Compton, says the company can expect a large fine for its negligence.

A report from Accenture suggests that, despite higher levels of investment in advanced cyber security technologies over the past three years, less than one-fifth of organisations are effectively stopping cyber attacks and finding and fixing breaches fast enough to lower their impact.

The government introduced a new Fire Safety Bill, which amends the Fire Safety Order 2005 to clarify that the responsible person or duty-holder for multi-occupied, residential buildings must manage and reduce the risk of fire for the structure and external walls of the building, including cladding, balconies and windows; and entrance doors to individual flats that open into common parts.

Weinstein and the workplace

The recent Harvey Weinstein trial and verdict are landmarks of cultural and legal significance, Edward Henry QC argues. Those in positions of authority, as well as compliance, risk and HR professionals should heed its warning

Harvey Weinstein's dramatic fall reminded me of Ernest Hemingway's description of bankruptcy. It happens "gradually and then suddenly". Gradually, because the allegations, once they emerged in 2017, had stripped him of the pervasive power he once enjoyed. He was perceived (and perception is important) to be no longer invincible. Following the revelations of harassment and sexual misconduct, more and more women felt able to come forward to speak about their experiences at his hands. Then came the trial, constructed on the premise that his coercive and domineering personality, allied to vast power and privilege, enabled him to control his victims. As in his days of pomp and fame, so it was in his downfall: denial and disbelief that anyone could accuse him of anything.

When the verdict was returned, his stunned expression was accompanied by him mouthing the words "but I'm innocent". Many of us had anticipated that moment, but the endgame was as sudden and brutal as the crimes he was convicted of. Shortly afterwards, Cyrus Vance Jnr, the embattled District Attorney who brought the case, told reporters, "It's a new day because Harvey Weinstein has finally been held accountable for crimes he committed."

Some might disagree with Vance. Some would say that Weinstein was convicted not for the offences upon which he stood trial, but was instead condemned for the infamous multitude of time-barred allegations that could never be brought to court. Such speculation can be objected to on the precisely the same grounds that Donna Rotunno, his attorney, faced criticism. Like her aggressive cross-examinations, this theory fails to take on board the dynamics of power, placing too much reliance on old stereotypes of sexual behaviour, whilst assuming that matters of consent are binary in nature, unqualified by ambiguity, or even regret, and simply a question of yes or no. This has important implications for those who owe a duty of care to their co-workers or subordinates. The two victims in the trial had complicated and difficult stories to tell, replete with contradictions, and inconsistencies, which made them vulnerable to attack in cross examination. Their accounts, which might be considered bizarre and at times unconvincing can only be understood when one recognises the immense power Weinstein wielded. "He did not invent the casting couch" (his previous attorney's quip to laugh the case out of court) but his omnipotence in the film industry was such that his victims were placed in a position (for all their acquiescence) of duress, paralysed by the fear that he would annihilate their careers.

There were, inevitably, a number of 'easy wins' for the defence. For example, both women made no attempt, physically to resist his advances, each kept in contact with him after the attacks, and they even had consensual sex with him in the months that followed. This is not evidence that usually accompanies a conviction, but it would be wrong the suggest that the jury convicted because of sympathy or prejudice. In fact, their decision reflects a degree of discriminating judgement, and sophistication, which reflected the complexities that underly human sexual behaviour. These verdicts can therefore teach us a lot about why conduct and culture in the workplace has changed, and must change still further. A discerning observer will take away from this trial the necessity of seeing the 'warning signals', and giving proactive guidance on risk, by paying more than mere lip service to a cultural shift in our society.

Where there is inequality of power, or status (classically found in the film industry, but existing whenever an unequal relationship of employment, tutelage or authority exists) one must acknowledge that consent is not the same as submission. That absent real equality, there is a danger of exploitation. In consequence, behaviours which were once tolerated and seemingly welcomed, must now be carefully scrutinised. The classic example is the drink fuelled office party. Anything untoward happening in the workplace or its premises (whether or not at a social gathering) can clearly be the subject of both employment and disciplinary proceedings. And what of behaviour outside the usual ambit of work, between colleagues? Should conduct

outside the workplace become the subject of regulatory investigation and disciplinary proceedings? In the context of the legal profession this is a novel development. On one side of the debate there is the argument that regulators have a duty to uphold confidence in the legal profession, but there is the concern that the SRA may be encroaching far too far into the lives of those they regulate, placing increased pressure on law professionals. The question arises as to what is to be reasonably expected of legal professionals, or should they be held to a more onerous sense of propriety? Where does one draw the line, ensuring that standards are upheld, whilst acting proportionately so as to avoid unreasonable intrusion?

A recent example of the problem concerned a former 'Magic Circle' partner who was fined £35,000 plus £200,000 costs for professional misconduct after he went back to the home of a junior colleague following post-work drinks in 2016. The SRA alleged he had initiated and or engaged in sexual activity where he ought to have known his conduct was unwelcome and that the other party was intoxicated to the extent she was vulnerable with her faculties impaired. The SDT on 30th January 2020 found he had caused harm to the profession by breaching his obligations as a solicitor but posed no future risk to the public. He was not struck off and thus allowed to keep practising. The SDT said his misconduct was the result of a "lapse in his judgement that was highly unlikely to be repeated." The decision pivoted on his duty of care to a more junior colleague. In reaching this conclusion, the SDT rejected arguments that the case was an unwarranted incursion into the lawyer's right to privacy.

It is important to stress that no finding on consent (or lack of it) was made by the SDT, as the SRA did not seek to establish whether consent was given or not, yet another aspect of its case that drew criticism from those representing the lawyer, who argued that if the complainant had consented he should not face any proceedings at all.

"It seems undeniable that the Weinstein scandal had a causal effect in prompting some businesses to implement preventative strategies to avert such risks"

The matter is currently being appealed, but even if the original finding is ultimately set aside, it shows that regulators, especially in this post-#MeToo world will pursue such cases vigorously, with an impact on reputation management, D&O premiums, and employment claims. The aggressive approach of the SRA follows in the wake of other regulators, such as the GMC. It seems undeniable that the Weinstein scandal, unleashing the huge power of the #MeToo movement; leveraged by the digital media, had a causal effect in prompting some businesses to implement preventative strategies to avert such risks, or (in crisis mode) to act ruthlessly in order to neutralise the entwined threats of outraged departing customers, and a collapse in share value. Take, for example, Ray Kelvin, the hugely respected designer and retail guru, having to stand down at the helm of Ted Baker in 2019 because of myriad claims concerning the alleged touching and hugging of staff. The brand, which was almost synonymous with Kelvin, was in imminent danger of being severely damaged. Corporates are therefore increasingly aware of the destruction such allegations can inflict upon their capitalisation. In the past, complaints would routinely be caught and killed with severance packages, compromise agreements or NDAs. Not anymore.

This is unsurprising after these strong arm tactics came under the parliamentary spotlight. Parliament in its 2019 Report on the use of NDAs in discrimination cases took a dim view of them, stating that, while it is usual for each party to pay its own costs in the UK, tribunals may only make costs orders requiring one party to pay the other's costs where there has been "unreasonable conduct", but such orders are rare. Citing Professor Dominic Regan's evidence that "pressure can be exerted on claimants by threatening to pursue costs if an offer was not accepted and, at the hearing, the claimant recovered less," Parliament noted that whilst the use of such tactics should be less common at tribunals, it had "heard that such threats are being used, even though they may be unenforceable. Claimants who do not have legal representation may be particularly vulnerable to such tactics."

Sexual misconduct is a serious issue and vigorous action is needed to alter behaviour and instil a culture of respect. This begins by creating an environment that safeguards and upholds common values, and by challenging sexually motivated misconduct from the outset. If litigation, regrettably, cannot be averted, it might be advisable to conduct it in a manner that does not alienate the tribunal, without compromising the proper defence of any contested allegation.

Edward Henry QC, of QEB Hollis Whiteman, defends in serious fraud, professional disciplinary and regulatory offences, and has an AML advisory practice. For 17 years he acted as a pre-publication advice lawyer for Associated Newspapers and has a keen interest in reputational management.

From chaos to continuity

The severity of the ongoing lockdown is forcing businesses to operate in ways that might transcend even the most frequently war-gamed scenarios. Deborah Ritchie reports

In getting to grips with the unprecedented measures taken by governments around the world as they attempt to control the COVID-19 virus, it is safe to say that the last few weeks will have been an operational challenge for most organisations.

The tension between mitigating health risk and keeping the country 'open for business' has led to heated debate around Boris Johnson's models and policies, and on the rights and wrongs of his government's decisions – decisions which have triggered a significant economic shock, the full extent of which is unknown.

The pressure is already bearing down on businesses across a wide range of industries and sectors. The decline in second-quarter GDP is expected to be considerable, with travel, retail and hospitality bearing much of the brunt. The capacity of organisations to manage the operational and people risks is hugely varied; some are simply more prepared than others.

Business continuity industry veteran, Mike Osborne, says that while the sheer scale of the impact is unprecedented, the UK's history of emergency preparedness in responding to threats and incidents over the last 50 years makes the country far more experienced and better prepared than many others – particularly with the now added availability of high-speed networks and cloud computing. At the same time, he believes this experience could change businesses forever. "One thing my business continuity experience has taught me is that firms very rarely go back to being exactly as they were – this experience will fundamentally change business IT, working practices and processes," he opines.

Amongst those businesses, some will have invoked tried and tested crisis management and contingency plans, others will have dusted off a plan that's not had the necessary attention or buy-in for however many months, and the rest will have just hit a very steep learning curve.

Regardless of where on that scale a business finds itself, the following perspectives may offer a refreshing view on how best to navigate this unprecedented time.

An IT continuity practitioner's perspective

From an IT perspective, correct purchasing and contracting of infrastructure should not be underestimated. The ability to flex services as and when you need to, rather than being tied into stringent contracts for the cost benefit, could make or break a business in the context of COVID-19.

If you have gone to the trouble of purchasing IT services to provide resilience, it's important they actually do that. Some companies may think they have that box ticked, only to find out too late that what they have bought does not actually meet their needs.

Take the example of a City firm which recently purchased adequate VPN licenses for everyone in the company, overlooking the fact that just a fifth of them could be used for remote working as part of the licensing agreement. To their credit, this was discovered during testing, so the model could be fixed ahead of the event.

Having the correct number of concurrent remote connections is one thing, but if the networks the VPNs are trying to connect to don't have capacity in the bandwidth, the user experience will be severely degraded. It's not until you actually have live demand on your bandwidth that you can accurately assess whether your infrastructure is truly resilient.

Success when you most need it depends on a few key things. Most of them are clichés in our world but really do deliver your recovery for you.

Familiarity People knowing how to work from home without needing any support to do so – already having the kit, knowing how to use it, working remotely on a regular basis and being comfortable doing so.

Trained people Those engineers who look after our systems need the ability to be able to identify and rectify problems quickly, and be able to failover manually if automatic failover is unsuccessful. They also need to be able to do all of this remotely.

Trusted suppliers This comes back to the earlier point about purchasing. Lots of companies try to drive as much value as possible from their suppliers, however relationship management pays dividends when there are many companies vying for

attention – such as at times like this.

Resilience by design If you want to be resilient, you do need to invest. There is no getting away from this. Having good infrastructure architecture is the basis for good IT provision.

No matter how well prepared you are as a business, there will always be people who are reluctant or technically challenged to work remotely. Allowing for a reduction in productivity when planning for longer-term remote working is not a bad idea. Some people will be more productive at home, but this will be negated by those who are not as disciplined (probably because they don't often work remotely).

Finally, it is worth managing users' expectations about what their experience will be like when they're connected to corporate systems at home. People expect that the speed and service of, say, video conferencing will be exactly the same at home, not realising when they're in the office they're on an enterprise-grade network with significant bandwidth. Trying to video conference with Asia on a 17mbps copper wire broadband is not going to work as well.

The business continuity consultant's perspective

Les Price, head of availability services, Daisy Corporate Services

The scale, speed and severity of the COVID-19 threat is far greater than that of previous pandemics we've experienced, and response measures across the board have been scaled up accordingly. The UK has not seen this level of event since World War II. We have panic buying, infrastructure closing, lockdowns... the level of risk is unparalleled and the knock-on effects are where the biggest risks will ultimately emanate.

Since the last pandemic, we have experienced a change in the use of our dedicated work area recovery services, with many customers using their suites frequently and for various reasons, not just for emergencies. This has contributed to a better, more organised response from customers who are now using our services to split critical teams.

Even the most well-prepared organisations are on the brink of the great unknown – it is unlikely many organisations have tested their remote working capability to the extent of having all staff working from home for an extended period of time.

IT departments will need to ensure all devices are monitored to keep users and the company infrastructure safe, as well as working to ensure the technology is delivering the expected levels of productivity for the business. It's inevitable that cyber criminals will take advantage during the outbreak, and we predicted that huge increase in the number of attack vectors caused by home working, disrupted processes, quickly introduced IT systems and so on. Security, therefore, is going to be a major focus throughout the pandemic.

Just how resilient companies are in the UK when it comes to IT continuity challenges of this magnitude, we will soon find out. From our experience, it's likely to be a mix of success stories, epic failures and muddling-through. I see this hinging on four core factors. Firstly, the maturity of the organisation's business continuity management planning. Secondly, the organisation's stage on their digital transformation journey. At this point in time, to illustrate these factors, we have our availability services teams busy working with our contracted business continuity customers while the rest of the business works to deliver technology and solutions to those businesses who are less-prepared. Thirdly, the element of time. Unlike most disruptions where a percentage of business-critical staff can sustain operations for a given time, there is a concern that we are potentially facing months of disruption, and an organisation's resilience will depend on how well they will be able to manage and embrace change and adapt. This will literally be something that only time will tell, but experience of long-term invocations has shown us that the more time passes, the harder it is to keep control of the business and sustain values, culture and ultimately, revenues.

Lastly, the most important factor is people; this is also the most intricate, sensitive and unknown element. We are all dealing with the threat of COVID-19 on an individual level; no two people and their environments and experiences will be the same. Multiply this uncertainty by the number of staff you have to get an idea of the impact.

The insurance law perspective

Heidi Lawson, partner and Paul Moura, associate attorney at Cooley LLP

With the coronavirus, COVID-19, already taking its toll on the economy, are there any existing sources of insurance coverage to help cover the inevitable financial loss? With major sporting events, conferences, cruises and other excursions being cancelled as a result of the outbreak, including the cancellation of the 2020 Olympics in Tokyo, can a company look to its existing insurance portfolio and find any insurance coverage to help minimise the financial impact?

Traditionally, the most direct way to get insurance coverage for a disease outbreak is to obtain event cancellation coverage for events

cancelled or adversely impacted as a result of a disease or quarantine. To the extent a company purchases event cancellation insurance, events cancelled due to disease or quarantine may be expressly covered (or, in the case of very broad all-risk event cancellation coverage, not excluded).

However, without event cancellation coverage, most companies will need to hunt around for other possible sources of insurance. Political risk insurance, which many companies may already have due to international investments or overseas operations, may cover losses as a result of a government shutdown or curfews.

Unfortunately, with many political risk policies, this form of indemnity often necessitates a waiting period of 90 days or more prior to coverage activation. By the time the political risk policy takes force, there may be no need for it anymore.

Similarly, civil authority clauses in first-party policies can afford coverage for business income losses that arise when a civil authority prevents the policyholder from accessing their premises, which may happen when a civil authority blocks access to a property facing an outbreak. These coverages also typically have waiting periods (eg. 72 hours) before coverage can be triggered. Notably, such coverages will often depend on whether there is a requirement of physical loss, which may not be present in the case of an outbreak.

Directors and officers insurance coverage may apply if investors or customers eventually sue a company and its directors and officers as a result of losses incurred from breaching a quarantine or failing to take timely or appropriate action to mitigate the impact of a disease, resulting in additional sickness, a company shutdown and, eventually, lost revenues as a result. However, one important thing to note is that many D&O policies have a broad bodily injury exclusion. As a result, coverage under a D&O policy depends on the precise policy wording and underlying facts.

Finally, another potential source of insurance might be under a company's employment practice liability insurance. EPLI can sometimes assist companies involved in actions by employees because of layoff or furlough claims due to government or company shutdowns.

To the extent that existing policies currently provide coverage, either directly or indirectly, we can expect that the insurance market will react quickly and add additional exclusions for disease or quarantines to many existing insurance policies, at least until the current outbreak subsides.

Pandemic planning

Roger Kember is former Deputy Director of Capabilities in the Civil Contingencies Secretariat, since the very first week of its existence. He instigated the Department of Health Pandemic Plan in (2001) and also wrote the national police pandemic plan. For 17 years, Roger also managed the police room in COBR. He is now a crisis management consultant.

When the Department of Health published its first UK Influenza Pandemic Preparedness Plan in 2001, the risk was based only on the flu virus, with the 50 million plus deaths worldwide from the Spanish Flu Pandemic of 1918-19 the worst-case benchmark. Seasonal flu will always be with us as well as spikes from new strains of the flu virus, as in 2008-09. We are still waiting for the 'big one' (expected to be a variant of avian flu), so, the 2001 Plan (including its slight revisions over the years) will still hold good.

Scientifically, the coronavirus is different from the influenza virus, but these two viruses have as many differences within themselves as between themselves. We've had mild flu outbreaks as well as severe ones. The coronaviruses SARS and MERS had high mortality rates but did not spread worldwide as the variant responsible for COVID-19 has.

These differences are important to doctors but to business continuity professionals, businesses and other organisations, the impact of a pandemic (whatever the virus) is the same: human beings are quarantined, ill, recovering, caring for family or succumb to the infection.

Taking so many people out of circulation at the same time and all around our interconnected world has a significant business impact on production, logistics, services and markets. It also has social, personal and family impacts both practically and psychologically. Many businesses say that 'our people are our most important resource': a pandemic tests this statement to the limit.

This outbreak is characterised by the definition of a 'crisis': "An abnormal and unstable situation that threatens the organisation's strategic objectives, reputation or viability." (Crisis Management: Guidance & Good Practice BS 11200).

Medically, it's a new virus; there's no vaccine; its lifecycle is only partially known; viral shedding (infectiousness) can last for 24 days (ie. 10 more than the government advised quarantine period) and we don't know if it will mutate (like 'flu) and hit us with a new variant every year.

Business-wise, the world is a very different place today compared with 2001, so the learning from past flu pandemics is only a partial help.

Businesses have suffered the triple

blow of a supply crunch, a demand slump and a cash-flow constriction.

This has been the first pandemic to hit the world after China has earned itself the moniker of 'workshop of the world'. Globalisation of supplies and cheaper costs there have made the world dependant on it for a range of goods, from electronic components used in ventilators to hand sanitisers. China is the largest manufacturer of generic drugs and produces 80 per cent of the world's basic active pharmaceutical ingredients. India is the world's second largest producer of generic drugs but imports 75 per cent of its APIs from China.

Demand for everyday groceries has spiked due to stockpiling but demand has slumped to near-zero in the tourism leisure and hospitality sectors and associated industries of airlines, credit card companies, breweries and professional catering supplies. So long as self-isolation continues, so too will the demand slump.

No sales equals no income. Every bankruptcy leaves bad debts. Staff layoffs result in reduced demand from consumers, which means reduced sales and reduced cashflow. This is where the world economy was in the Great Depression. Fortunately, present governments are following Keysian economics and have declared they will pump government money into the economy and suspend some tax burdens from businesses for the time being. There is not yet complete clarity on how some of these will be put into effect and it is still too early to determine if these provisions will be sufficient.

There are a number of 'firsts' associated with this pandemic.

China as the workshop of the world and the knock-on problems of supplies and the logistical movement of shipping containers. (China has made a number of strategic decisions on trade including its programme to become the world's dominant maritime nation and maritime insurer). Indigenous industries in the west have largely gone to the wall unable to beat China's pricing policies. For many products, we have no UK suppliers. We have a chronic shortage of personal protection equipment for the health service, care workers and others on the COVID-19 front line.

It's the first to hit the UK after its 'Cold War Dividend' changed the government's strategic thinking. Until the fall of the Soviet Union, the UK (and ATO countries) protected its strategic industries: principally the defence sector, but also the security of government communications networks. With the end of the Cold War, the government decided there was no longer any threat to the UK and drastically reduced its subsidies and funding to these defence-critical industries.

We are now in the age of social media. It is being used by the government to get its infection control measures out to the public and official guidance is available everywhere online. Social media is also being used to overcome the loneliness of self-isolation. Local community support groups are using Facebook and other apps to keep in touch with those who may need help and support. The flip side is the scammers and conspiracy theorists are already at work. A crunch point will come if the number of patients needing ventilator support vastly exceeds the ventilators available and people die who otherwise might have been saved. The burden will fall on doctors to decide who lives, and that will be impossible to keep off social media.

Working from home has become a fact of business life. It may even become a mainstream feature in the same way that open-plan offices and hot-desking has been factored into cost reduction. With schools, colleges and universities closed, it will be a full-load test of the domestic broadband capacity with users streaming, playing interactive games, Skyping/Zooming and downloading while others are trying to connect to work servers.

The fifth element is the government's issue of emergency powers, how these will be enforced and what the public reaction to them might be. In crisis management, it is always wise to undertake some 'worst case scenario' planning. My potential worst cases are:

- This coronavirus will return in waves (the Spanish Flu had three waves)
- It mutates, like the flu virus, and will threaten the world with a new outbreak (of unpredictable severity) every winter
- We get a flu pandemic and coronavirus pandemic at the same time
- We suffer a different crisis at the same time (eg. solar flare, flooding, oil shortage, extensive cyber attacks or major military confrontation).

Everyone is doing their best to deal with this situation using their existing pandemic plan and there is a lot to do on a day-to-day basis. Everyone will need a coronavirus pandemic plan as well as their flu plan. Make the time now to take stock of your pandemic response and coronavirus business continuity plan and revise them in the light of your experience to get effective day-to-day management (ie. 'command and control) and give top management the head room to consider the strategic issues for now and the post COVID-19 world.

Deborah Ritchie is group editor of CIR Magazine

Eastern horizons

The Middle East has proven to be a politically volatile and unpredictable part of the world but remains a crucial region for many firms. Balancing risk and opportunity is as important now as ever, writes Martin Allen-Smith

- Where are the next risk hotspots in the Middle East, and how can organisations best prepare for the often dramatically shifting sands in there?
- Carrying out comprehensive due diligence and having a full understanding of your operating environment – the site, the country, the region – is key
- Longer term, the IMF warns that without widespread reforms, the region's oil wealth could vanish as early as 2034 as global demand for oil slides

By any standards, 2019 proved to be a turbulent year for doing business in the Middle East. Several countries were shaken by unrest and protests, there were increased and very significant risks to international shipping in the Strait of Hormuz, the Syrian civil war continued relentlessly, and, indeed the most worrying of all at the time, there was the very real threat of conflict between the US and Iran.

Against this backdrop of ever-changing political landscapes, where are the key hotspots in the Middle East to have proved a particular challenge from a risk management perspective – and how can organisations best prepare for the often dramatically shifting sands in these areas? It is fair to say that the Middle East and North Africa has the full gamut of risk environments, like other regions – from low risk jurisdictions like Morocco and Jordan, to extremely high-risk countries like Yemen and Syria. Operators and underwriters with exposure in those facing political stability challenges like Iraq and Lebanon need higher risk thresholds than elsewhere, says Niamh McBurney, head of MENA at Maplecroft.

"Amid often fast-paced events, it's important to clarify what is new in the situation and then assess how it relates to you. A change in government will not always bring an immediate change in regulations, and political instability or civil unrest doesn't necessarily prompt business disruption," she explains.

"Concerns about political violence are highest in Africa and the Middle East, with concerns around how technology, such as drone strikes, could exacerbate the risks"

"For example, protests in Egypt in September 2019 were small, contained and did not disrupt business operations. Short-term exposure to an asset in Yemen might seem like a risky bet – unless you know that the asset's location has not been materially affected by the civil war. Doing your due diligence and having a full understanding of your operating environment – the site, the country, the region – is key."

She adds that Iraq offers rewards to those willing to take big bets on risk management and Egypt's restructuring of its economy between 2016 and 2019 was challenging for those exposed to the banking sector – effectively all foreign operators, investors and underwriters.

Organisations doing business in the region need to have a comprehensive mix of knowledge and flexibility if they are to ensure that they are in a position to act quickly should political tensions arise in a particular country or region.

If political tensions look like they could become disruptive, securing their assets – whether physical or financial – clearly comes first. But organisations need to know the local laws first to do that effectively. It is one thing to understand the past, and another to know the future, says McBurney. "Knowing the history of confiscation, expropriation, nationalisation and disruption (CEND) combined with a deep understanding of local political dynamics allows you to assess how risks to your assets will change. Take Lebanon's recent sovereign bond default – its credit history would suggest it would successfully repay to foreign bond holders and their underwriters, but looking closer into the political dynamics right now, politicians were not willing to repay international lenders at the expense of the domestic banks, because it would hurt friends and family members of the political class.

"Geopolitical or regional events, political spats or pivots in alliances, most often lead to very subtle changes for those on the ground, but being aware of those changes can be the difference between an opportunity and a loss later on."

The wider political risk landscape is becoming more precarious,

according to the results of a survey by Willis Tower Watson. It asked 41 major corporations for their take on the global picture and the general view was that such risks had increased during 2019. Disruption of international trade was considered the most significant risk in the majority of regions. Fifty-eight per cent of respondents cited trade sanctions as a concern for their operations in Europe, 67 per cent in Asia-Pacific, while for Russia and The Commonwealth of Independent States (CIS), the figure was 77 per cent. Concerns about political violence were the highest in Africa (74 per cent) and the Middle East (71 per cent), with respondents reporting that new technologies such as drone strikes could exacerbate such risks.

2019 also saw an increase in the proportion of companies reporting that they had experienced political risk losses, according to the research. 54 per cent of respondents had experienced a loss due to political violence, compared with 48 per cent in 2018. Some 46 per cent reported losses due to trade sanctions or import or export embargoes in 2019, compared to 2018's figure of 40 per cent. Almost a third of companies with revenues exceeding US$1bn reported previous experience of a catastrophic political risk loss of more than US$250m.

"It is clear that political risk continues to increase, and that related financial losses are on the rise," says Paul Davidson, chairman of financial solutions at Willis Towers Watson. "Corporations now face a strategic choice: to either maintain their global business models while accepting,

"Iraq offers rewards to those willing to take big bets on risk management"

"Egypt's restructuring of its economy between 2016 and 2019 was challenging for those exposed to the banking sector – effectively all foreign operators, investors and underwriters"

mitigating or transferring the political risks associated with them, or attempting to realign themselves with the emerging shape of a new and apparently more nationalist global landscape."

The majority of respondents (71 per cent) stated that emphasis on political risk management at their company had increased since 2018, and nearly 40 per cent felt that they were facing more pressure from investors regarding political risk management. The study included in-depth follow-up interviews with a panel of survey participants, whose top risks of concern included Middle East regional stability, alongside US-China strategic competition and the potential for an environmental/social/governance shock.

Of course, no region sits in isolation, and the situation in the Middle East often reflects the worldwide geopolitical risk landscape. So how have recent global shifts affected things, and where does the Middle East currently sit compared with other regions in terms of risk and complexity?

Certainly the ripples of domestic and foreign policies of the US, Russia and China all have an effect on the Middle East. Maplecroft's McBurney believes that changing US policy towards the Middle East was one factor in Gulf states like the UAE and Saudi Arabia increasing the share of their oil exports to China and other major Asian consumers: "Combined with the boom in domestic tight oil production, the US now considers itself effectively energy independent – an extraordinary change from just a few years ago which robs the Gulf states of a market and reduces US exposure to the region. Robust governments without fully democratic systems provide more stability in some ways than in other regions like Latin America."

There remains long-term concerns over some of the economic conditions that have made some gulf states such attractive propositions in the past. The International Monetary Fund warns that without widespread reforms, the region's oil wealth could vanish by 2034 as global demand for oil slides. It suggests that some of these oil-rich countries will need to rationalise spending, reform their large civil service sectors, and reduce public wage bills – all of which could be delicate issues that risk having an adverse affect on citizens who are more accustomed to subsidies and low taxes.

But McBurney adds: "The underdeveloped regulatory environment and extensive presence of government-owned businesses in key sectors makes the region less dynamic – but this is starting to change. The region's position in the energy supply chain and increasingly in the renewable energy sector means it will continue to be influential for the next several decades."

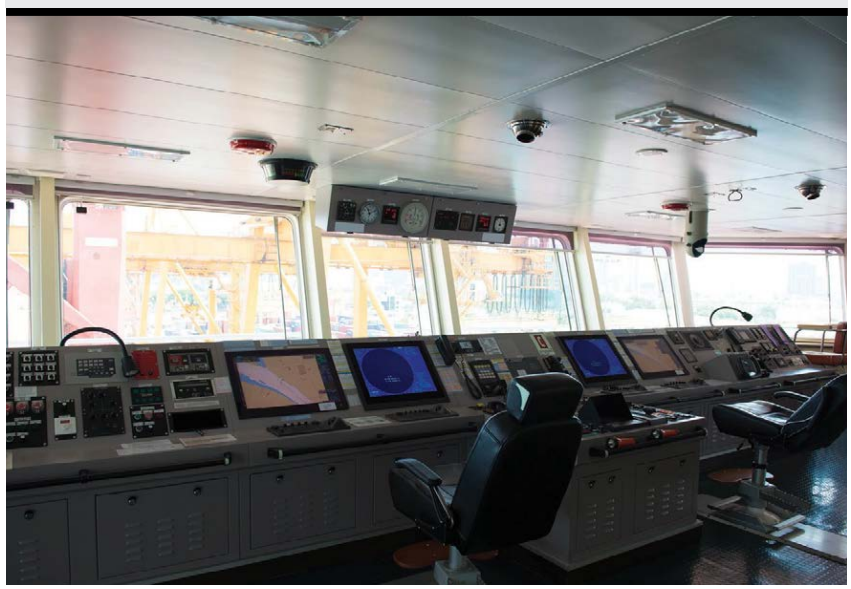
Of course, no-one knows yet how any of the conventional norms will be transformed in a post-COVID-19 world, but it is likely that, despite the risks, the Middle East's role as a pivotal business focal point for many global organisations will remain for a long time to come.

Martin Allen Smith is a freelance journalist

Adjusting course

An increased trend towards and reliance on interconnectivity brings a heightened risk of cyber attack or systems failure for the maritime sector – and the supply chains it serves. Ant Gould reports

- The global maritime community is increasingly embracing interconnected technologies across shipping, shipping company and port systems
- Whilst greater efficiency, safety and transparency are all welcome, the ever-present threat of cyber attack or downtime cannot be overlooked
- Efforts to manage these risks include a raft of new guidelines and regulations, with the deadline for the new IMO rules now clear on the horizon



The global maritime community not only faces the same risks as any business, but has now to consider the risks relating to increasingly digitalised on-board operational technology and greater interconnectivity between shore-based and on-board systems covering navigation, propulsion and power control. And with autonomous and semi-autonomous vessels coming onto the horizon over the next few years, the risks can only increase.

2017 was a pivotal year in terms of the marine sector's awareness of, and response to, the cyber risks it faces. Maersk's cyber incident, where the shipping giant's systems were taken offline, globally, for nearly two weeks, represented a major wake-up call. The NotPetya malicious malware code entered Maersk in the Ukraine via its accountancy systems and rapidly spread across the organisation, disabling 49,000 at 600 sites across 130 countries.

That same year, the International Maritime Organisation issued guidelines on maritime cyber risk management. They contain high-level recommendations designed to safeguard shipping from current and emerging cyber threats and vulnerabilities and include functional elements which aim to support effective cyber risk management.

The IMO also gave their ambitions some teeth and passed a resolution which "encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems no later than the first annual verification of the company's Document of Compliance after 1st January 2021". So, the clock is ticking on operators.

New threats, new guidelines

The comprehensive IMO guidelines cover digitisation, integration, and automation of processes and systems in shipping. They also identify bridge systems, propulsion and machinery management, power control and communication systems among the most vulnerable to attack.

In the wake of Maersk and the IMO move, awareness across the industry of the threats it faces has certainly increased. And as the Baltic and International Maritime Council (or BIMCO as it is now known) says, conversations have evolved from awareness to preparedness, and a host of supporting initiatives have been launched to support this journey.

The UK government for example produced two comprehensive guides, to both ship security and cyber security for ships which are regularly updated.

The former guidance, produced by the Institution of Engineering and Technology, includes advice

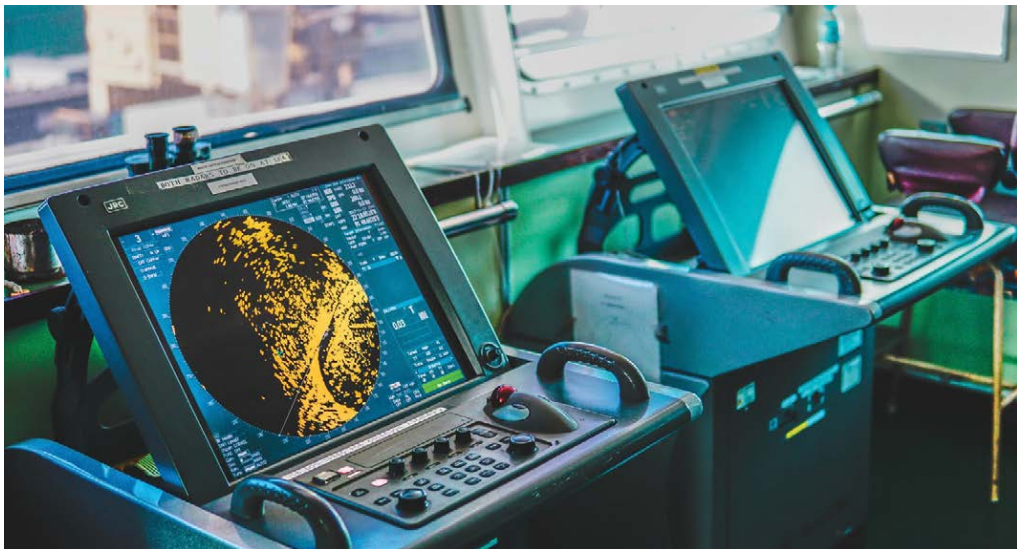
on developing a cyber security assessment and plan, and handling security breaches and incidents.

The latter, the ship cyber security code of practice, also produced by the IET with the support of the Defence Science and Technological Laboratory, provides actionable advice on developing a cyber security assessment and plan to manage risk handling security breaches and incidents highlighting national and international standards used.

Across the sector, guidance and guidelines are now in abundance. At the beginning of last year a joint initiative by shipping industry bodies BIMCO, the International Union of Marine Insurance, Cruise Lines International Association, the International Chamber of Shipping, Intercargo, Intertanko and Oil Companies International Marine Forum resulted in the publication of the third version of the Guidelines on Cyber Security Onboard Ships. This comprehensive document – which uses the National Institute of Standards and Technology (NIST) framework – offers guidance to shipowners and operators on how to assess their operations and develop the necessary procedures and actions to improve resilience and maintain integrity of systems.

The guidance looks at incorporating cyber risks in a ship's safety management system. It also reflects a deeper experience with risk assessments of operational technology – such as navigational systems and engine controls – and provides insights into dealing with the cyber risks to the ship arising from parties in the supply chain.

As more and more operational technology is integrated with information technology and connected to the internet,



risks increase – and change. Malfunctioning IT may cause significant delay of a ship's unloading or clearance, whilst malfunctioning or inoperative OT there can be a real risk of harm to people, the ship or the marine environment.

Dirk Fry, chair of BIMCO's cyber security working group comments: "On a ship, the job may be less focused on protecting data while protecting operational systems working in the real world has direct safety implications. If the ECDIS [electronic chart display and information] system or software controlling an engine are hit with malware, or if it breaks down due to lack of compatibility after an update of software, it can lead to dangerous situations."

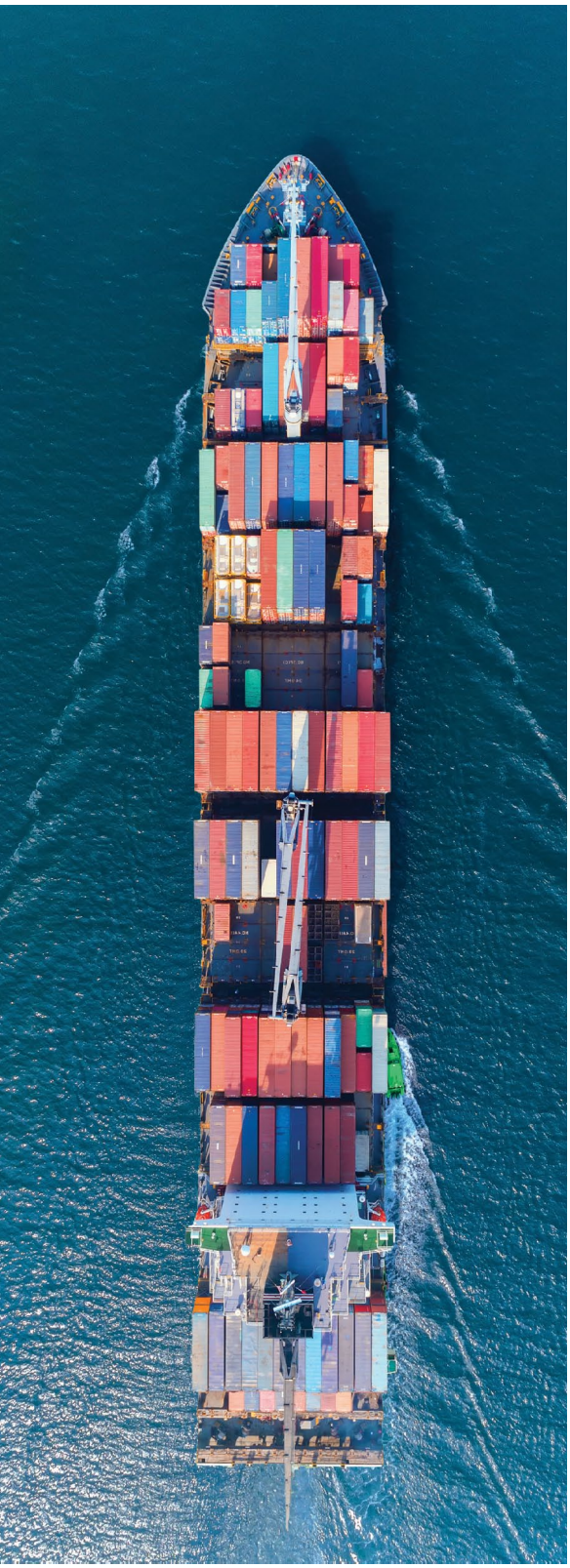
There is also an increased risk of malware infecting a ship's systems via the many parties associated with the operation of a ship and its systems, Fry adds . "The ships are not just sitting there in the middle of the ocean. More and more ships are also closely connected to security systems in the companies' offices and shippers' offices and agents' offices."

Advice in the guide includes evaluating the security of service providers, defining a minimum set of requirements to manage supply chain or third-party risks and making sure that agreements on cyber risks are formal and written. The guidelines also underline the need for ships to be able to disconnect quickly and effectively from shore-based networks, where required.

The human touch

Guidance and support have a role to play, but organisational response and resilience to cyber attack is as much about people and their behaviours as it is about technology or compliance. Humans are both the weakest and the strongest link, and with this in mind there have been real efforts to try and make sure crew at sea and staff on shore are vigilant and understand what to look out for and what mitigation actions they own themselves. This can be for example just being aware of the danger of spoof GPS signals and keeping a more traditional eye on the course of the ship.

Cyber awareness training is



essential but equally it needs to be effective and not just a tick-box exercise, as Lloyd's Register recognised when it partnered with Axelos Resilia Frontline. The LR Cyber Resilience portfolio addresses the 'human factor' and the need for sustained behavioural change to build an organisation's resilience to the growing threat of cyber attack.

Nick Wilding, general manager, cyber resilience at Axelos says its awareness training has been designed "to offer short, story-based, engaging training designed to develop and sustain more resilient behaviours across the workforce". Building a more vigilant and engaged workforce and a resilient culture is critical to the ability to better manage these risks, he says.

Early this year the maritime academy and training centre Aboa Mare and maritime cyber security specialist Deductive Labs also developed a new maritime cyber security training programme aligned to the IMO's regulations and guidelines. The first course, aimed as masters, chief engineers, officers and other ship personnel was run in February of this year.

For those on board, there is also a new very practical Master's Guide to Cyber Security, which whilst aimed at the master and officers on a ship is also useful to shipowners, ship managers, ports and their IT departments.

The guide, developed by BIMCO and the ICS includes checklists to support day-to-day cyber risk management on board a typical merchant ship and addresses human factors, physical security and IT with a focus on how to protect, detect, respond and recover from a cyber incident.

This guide focuses on both IT and OT systems and breaks down complex issues (network segregation, ECDIS security, etc) into manageable and easy to understand tasks. From password protection to the use of personal devices onboard, every aspect of digital life at sea is taken into consideration.

As the maritime sector gets to grips with the cyber threats it faces, demand for, and interest in insurance coverage is also on the rise. Insurers, in particular, have responded with a wealth of advice on proactive risk management and support in developing rapid response plans and recovery programmes.

Last year insurer Beazley launched a marine cyber policy and risk management service for shipowners and operators aimed at vessel owners and operators, to cover physical damage and loss of hire caused by a cyber attack.

At the heart of its offering is preventative risk management – including a self-assessment questionnaire; a cyber security workshop; and an on-board cyber survey, along with a call for operators to demonstrate compliance with the forthcoming IMO guidelines.

As the IMO deadline for the industry to get its house in order approaches, activity across the sector will accelerate this year – perhaps supported by the potential downtime inherent in restrictions created by the global coronavirus pandemic. And whilst the maritime industry is now awake to the cyber challenges it faces investment in staff training, the development of new approaches to assess and protect risk and recovery plans is crucial if it is to navigate the cyber challenges ahead.

Ant Gould is a freelance journalist

airmic

www.airmic.com

LIVE Webinars

COVID-19 UPDATES

www.airmic.com/airmic-live-webinars

Into the forest

Despite the global sigh of relief when rain fell on Australia's bushfires, the damage had been done, and will take time and resources to fix. Jeremy Hughes counts the cost to the economy and to the insurance industry

- The recent bushfires in Australia touched the whole world, their societal and ecological impacts difficult to perceive and to quantify
- The damage to property and businesses can to some degree be measured and recovered – with insurance claims so far expected to be manageable
- Previous significant fire seasons cost A$1.8 bn (£894 m) for the Black Saturday fires, A$2.5 bn for Ash Wednesday and A$2.16 bn for Black Tuesday

Australia's recent wildfire season officially ended on 10th February, when heavy rainfall across most of the firegrounds finally extinguished numerous blazes, some of which had burned since before November. Focus had inevitably shifted to subsequent events, with recovery efforts largely escaping the intense coverage devoted to the dramatic height of the crisis.

Starting at the peak of a catastrophic drought and exacerbated by the resulting deep-seated aridity, allied with higher temperatures and high winds, the fires in Australia's New South Wales, Victoria, Queensland and Western Australia regions were labelled 'unprecedented' by a government struggling to mount an adequate response.

The climate numbers are clear: 2019 was Australia's hottest and driest year on record, with the annual national mean temperature 1.52 °C above average with nationally-averaged rainfall 40 per cent below the average for the year at 277.6 mm. In southeast Australia, hardest hit by the fires, 2018-2019 was the driest two-year period on record. Fires started earlier than usual and continued without pause – until heavy rains in February, there was every prospect that they would burn for many more months.

While the human toll of 34 people killed may appear relatively light compared to 2009's 'Black Saturday' toll of 173, 80 per cent of Australia's population suffered an impact in some shape or form, including 57 per cent from smoke, according to a poll by the Australian National University. And while the damage to property and businesses can be measured and recovered – to some extent at least – a range of fundamental societal and ecological impacts are more difficult to quantify and may signal permanent changes to the country and its perception of itself.

"A high proportion of Australia's economy is at risk from natural disasters"

Measuring the tangible costs

By 13th February, the Climate Council estimated that the fires had destroyed nearly 6,000 buildings, destroying 2,439 homes and damaging a further 1,021 in New South Wales alone. More than 11 million hectares were destroyed: the final damage to private property could amount to between A$5 billion (£2.5 billion) and A$10 billion.

Before the fires, Australian agriculture was predicted to grow by more than A$3 billion a year to become a $A100 billion industry by 2030, ranking it with mining and construction as one of the country's vital activities. Final numbers don't exist for the total loss of livestock, but on Victoria's Kangaroo Island alone, 100,000 sheep and more than 25,000 cattle were killed. A comprehensive tally of the damage to agriculture remains uncertain, but it's clear that 2019's growth figure is likely to be severely constrained.

Even in areas the fires didn't reach, smoke caused harm: for the South Australia wine industry, Australian Grape and Wine Incorporated estimates the cost of smoke taint at $A40 million while the NSW Wine Industry Association sees it approaching $A100 million in that state alone, taking into account the slump in wine tourism. That appears conservative given that the cost of smoke taint from 2003's fires was estimated by Wine Australia at $A300 million.

Australia's economy relies heavily on tourism – estimated to represent 10.4 per cent of Australia's gross domestic product and 12.2 per cent of total employment in 2018. The tourism sector is set to lose at least $A4.5 billion as a result of the bushfires.

The cost of fighting the fires, in terms of deployed human resources, equipment, consumables (including vehicle fuel, fire retardant and water) has been estimated at $A2.2 billion, with the bulk of firefighting manpower supplied by volunteer forces which were required to stay in

the field for longer, and deal with fires of greater scale and intensity, than they had ever anticipated.

Indirect costs

Much harder to quantify will be the immediate and long-term impacts on Australia's natural environment. In New South Wales, the bushfires burned around 5.4 million hectares (roughly 6.82 per cent of the state) consuming around 81 per cent of the Blue Mountains World Heritage Area and 54 per cent of the ancient Gondwana Rainforests in New South Wales and Queensland. An estimated 800 million wild animals were killed by the bushfires in New South Wales, with a probable national impact of more than one billion animals.

Perhaps the most telling measure was published by Western Sydney University's Hawkesbury Institute, which calculated that the area burned in the 2019-2020 forest fires far surpasses historic records globally. In previous fire catastrophe years, only about two per cent of Australia's temperate forests were burned, but in 2019/2020, a shocking 21 per cent of these forests were burnt – far above any previous historic records.

In addition, the bushfires released between 700 million and one billion tonnes of carbon dioxide into the atmosphere, such that due to the fires' severity and ongoing climate change, replacing natural carbon stocks lost to the fires would cost in excess of A$1 billion – and if replacing lost carbon pushes carbon offset prices to European heights, the cost could amount to A$2.8 billion.

Responses

The Australian Federal Government's initial response was delayed to some extent by the country's political structure which places responsibility

for firefighting and disaster recovery onto the states and requires state governments to formally request federal assistance. On 28 December, the Federal Government promised A$6,000 to each volunteer firefighter working for or owning a small or medium business and on 6th January, Prime Minister Scott Morrison announced a further A$2 billion in additional funds for bushfire recovery. This came alongside the formation of a National Bushfire Recovery Agency. In addition, it pledged A$50 million for animal recovery. Morrison also pledged A$76 million in mid-January to help restore the tourism industry, with the money to come from the A$2 billion National Bushfire Recovery Fund.

New South Wales' Premier announced an inquiry into the fires on 30 January to review the causes, preparation and response to the summer's bushfires. The six-month inquiry will examine the underlying causes of the crisis, taking into account weather, drought, climate change, fuel loads and human activity, as well as preparations, responses, communications and coordination.

For the insurance industry, ahead of a full picture of the damage, the Insurance Council of Australia committed to maximising the speed of payouts to bushfire victims with insurers committing to prioritising bushfire claims. The ICA also worked with state government in New South Wales and Victoria to streamline cleanup initiatives, ensuring fair and equitable treatment for property owners. It also established local trades registers to deploy local builders and tradespeople in the reconstruction of their communities, providing jobs and boosting local economies.

Assessors were in the field early, with major insurers agreeing to cooperate and share resources so as to hasten the claims process. By 14th February, Insurance Group Australia reported that its assessors had completed 97 per cent of assessments "to make properties safe in the impacted areas".

In numbers

Between 8th November and 14th February, more than 23,000 bushfire-related insurance claims were made in New South Wales, Queensland, South Australia and Victoria, totalling an estimated A$1.9 billion. The vast majority of these claims (81 per cent or nearly 19,000 claims) were in

New South Wales. By comparison, Australia's previous significant fire seasons cost about A$1.8 billion for the Black Saturday fires (2009), A$2.5 billion for the Ash Wednesday fires (1983) and A$2.16 billion in 1967's 'Black Tuesday' in Tasmania.

Compounding these losses, storms starting on 5th February gave rise to further damage. Sydney saw 392mm of rainfall over four days – more than in the second half of 2019 and three times the average rainfall for February, leading the ICA to declare a disaster as insurers received 10,000 claims at an estimated value of A$45 million. On 20th January parts of New South Wales, Victoria and Australian Capital Territory suffered an extreme hailstorm, resulting in 69,850 claims at a cost of A$638 million. About 70 per cent of claims were for domestic motor vehicles.

Despite support from government and the insurance industry, claimants reported difficulties in lodging claims. *ABC News* reported that only 75 per cent of residents in bushfire affected areas had contents insurance, while for those whose homes were lost, proving ownership became difficult if the documentation was destroyed along with the home. Consumer advocacy organisation CHOICE stated that policy definitions were too complicated, leading to delays. "There is no standard definition of 'fire' in home and contents insurance. Of the 26 major policies CHOICE experts examined recently, we found problems with 70 per cent of the 'fire' definitions, and major issues with 25 per cent of policies." In a poll of the public, CHOICE found that more than 35,000 Australians agreed that when a fire damages your home, being able to claim upon your insurance should be a "straightforward proposition".

The ICA responded robustly to CHOICE, stating: "Household policies are responding appropriately to claims relating to the bushfires. No concerns about policy wording as suggested by CHOICE have been raised with the ICA." It concluded that it was "concerned that this...report may discourage property owners from deciding to be insured".

Funding the payouts

Although the level of damage to insured property is likely to be unprecedented, the Australian Prudential Regulation Authority is confident that general insurance can cope. To ensure that insurers are able to pay "all legitimate claims to their policyholders under all reasonable circumstances", APRA mandates minimum capital levels for insurers to hold, ensuring their resilience in times of disaster. The body shows that existing capital resilience is well able to cover current claims – particularly against the backdrop of a quieter 2018 and 2019 until the advent of the fires.

APRA adds that reinsurance's role will continue to play a key part in ensuring general insurance remains resilient, with its own function being to promote close engagement with overseas reinsurance groups.

Despite comfortable resilience levels, in the shorter term, earnings for insurers may take a hit: for example, for the second half of 2019 fire disaster claims at OUTsurance and Discovery dented parent company Rand Merchant Investments' earnings by 14 per cent, with increased strategic spending at Discovery adding to the fall. During the period OUTsurance's earnings decreased 12 per cent, with the 'devastating' bushfires in Australia severely impacting the company's claims ratio.

Similarly, QBE's results were hit by claims arising from the Australian bushfires when it reported an operating ratio of 97.5 per cent above its 2019 target range of 94.5 to 96.5 per cent. During 2019, QBE Insurance Group's net Australia-Pacific catastrophe claims jumped to A$193 million from A$106 million in 2018, driven by floods on Australia's northeast coast and the bushfires in the southeast. Unfavorable weather conditions also impacted its US crop insurance business.

Other insurers have yet to report on the period that includes the fire season but at the global level, many reported a successful Q4 2019 and full-year performance, with fewer major catastrophe losses to damage their numbers.

Worries remain for consumers

in disaster-affected areas, with the prospect of future fires and floods occurring more frequently and with greater intensity due to climate change. QBE stated that as its customers looked for increased disaster cover, higher premiums may make insurance unaffordable, "especially for customers in areas more exposed to weather-related events". Fears have surfaced of 'red zones' where properties are uninsurable due to the risk of fire or flood in Australia, with owners of properties subject to coastal erosion near Newcastle in NSW already reporting an inability to secure cover. This, coupled with banks' reluctance to issue loans secured on properties in these areas, threatens significant financial strain for homeowners and businesses.

In addition, the reinsurance market foresees greater difficulty in the future: Swiss Re suggested in its outlook for the market an upward trend in rates had to continue if the reinsurance market is to be sustainable – before the recent COVID-19-driven rate cuts reversed the trend. But with a coordinated approach to risk modelling and building resilience in infrastructure and systems, the global reinsurance market currently has sufficient capacity to manage the risks.

Longer term

Australia's largest general insurer, IAG released a report in 2019 which emphasised that Australia's coasts face increased risk of intense cyclones – pushing the annual economic cost of natural catastrophes to an estimated A$39 billion (US$27 billion) by 2050. IAG urged prioritising infrastructure capabilities, suitable land planning and appropriate building codes – measures that would also stand

"Significant airtime was given to the baseless notion that the fires had been caused by arsonists"

fire-damaged regions in good stead if implemented during the phase of rebuilding that already under way.

Accurate and sophisticated risk modelling will be required to keep pace with increasingly rapid changes in climate. It's clear that ahead of Australia's fires, the existing models didn't get it right. World Weather Attribution recently reported that its analysis shows global warming made the wildfires at least 30 per cent more likely, and that should global temperatures increase to 2°C over pre-industrial levels, the conditions that drove the fires would be at least four times more likely to reoccur.

In fact, IAG and SGS Economics & Planning estimated in 2016 that a high proportion of Australia's economy was at risk from natural disasters: 20 per cent of GDP and 17 per cent of the population were situated in areas at high to extreme tropical cyclone risk; 28 per cent of GDP and 25 per cent of the population in areas with high to extreme flood risk; and 11 per cent of GDP and 9 per cent of the population in areas with high and extreme bushfire risk. A greater emphasis on disaster mitigation would therefore prove fruitful. As far back as 2014, the Australian Government Productivity Commission concluded: "Governments over-invest in post-disaster reconstruction and under-invest in mitigation that would limit the impact of natural disasters in the first place."

Policy and politics

Perhaps the greatest shifts in Australia need to be broader-based than in the insurance industry alone. The latest fires sparked an angry debate between the incumbent Liberal government and the Labour opposition as ministers traded public blows as to the causes of the conflagration. The government of Prime Minister Scott Morrison was hesitant to acknowledge the links between climate change, the drought, and the fires. Significant airtime was given to the baseless notion that the fires had been caused by arsonists; a mistaken theory persisted that the high fuel loads sustaining the fires resulted from green activists opposing preventative burning. Morrison, who drew opprobrium by holidaying in Hawaii while Australia burned, resisted making the link to anthropogenic climate change, at least in part due to his government's high-profile commitment to coal mining as a long-term driver of economic growth for Australia.

As a result, confidence in the federal government declined from 38.2 per cent in in October 2019 to 27.3 per cent by January 2020. As mentioned, the statutory requirement for the states to request help from the federal government – and the debate as to whether this could and should be overridden – made for needless delays in coordinated responses. Morrison recovered some poise with his A$2 billion support package – but his critics await his full acknowledgement of the need to address anthropogenic climate change and get to work on policies that will go further in building resilience and diversifying the Australian economy.

Until then, Australian insurers face a growing need to evolve their product offerings to respond to the prospect of more frequent disasters in the 'Lucky Country'.

Jeremy Hughes is a freelance journalist

QBE. Prepared.

How can businesses build resilience in a challenging operating environment?

Visit QBEEurope.com/resilience to find out.

QBE
Business insurance

Sponsored by

QBE

CIR
CONTINUITY INSURANCE & RISK

Raising the ramparts *Following the outbreak of COVID-19, Chinese authorities were facing a steep rise in the number of patients needing urgent care. To address the issue, they built an entire hospital in just 10 days. Andy Kane examines the key risks, as he lifts a lid on the construction* *Page30*

New dimensions *Working from home was BAU for many, long before COVID-19, but, as Deborah O'Riordan writes, the unprecedented scale of reaction and government intervention in this pandemic creates an unprecedented human challenge* *Page 32*

COVID-19 Focus

QBE

Sponsored by

Raising the ramparts

Following the outbreak of COVID-19, Chinese authorities were facing a steep rise in the number of patients needing urgent care. To address the issue, they built an entire hospital in just 10 days. Andy Kane examines the key risks, as he lifts a lid on the construction

A little over a week after construction started, the two-storey, 366,000 sq-ft Huoshenshan Hospital in Wuhan began accepting its first patients. Three days later, China opened a second hospital in the city – the 1,600-bed Leishenshan. The two hospitals – part of China's battle with the coronavirus – were built in record time using prefabricated modules. This impressive feat of design, engineering and construction, is exceptional, but prefabricated and modular forms of construction are becoming much more prevalent, with important implications for risk and insurance.

Faster, safer and more flexible

Prefabrication can be as simple as manufacturing sections of walls or roofing, right up to complete modules that come with services plumbed in. These modules can be stacked together like Lego blocks to build multi-storey apartments and offices – two 44-storey tower blocks currently under constructed in Croydon, London, are set to become the world's tallest modular buildings. At the extreme, 3D printing technology is being developed to manufacture entire homes – a Russian company recently completed the largest 3D printed building yet.

Few buildings can be built as quickly and on such a scale as the two hospitals in China. However, the use of prefabricated and modular construction methods is expected to accelerate in coming years.

In the UK, prefabricated buildings are thought to be essential for meeting current government housebuilding targets and last year Japanese modular building pioneer Sekisui House agreed a deal with the government to build modular homes in the UK.

Prefabricated buildings are a faster and less resource intensive way to meet growing demand for new buildings.

Crucially, much of the construction work is carried out offsite. This means potentially less disruption for local communities and a safer environment for workers. The Huoshenshan hospital took just 10 days to build. Using traditional methods, a similar building could take many months, if not years to construct.

Building resilience

The two hospitals in Wuhan are a great example of how prefabricated and modular buildings can increase resilience. There are obvious applications in emergency response, such as field hospitals, temporary shelters or rebuilding quickly following a natural disaster, such as floods or major storms.

Modular buildings could also increase the flexibility of the construction industry, and therefore its resilience and ability to respond to the needs of society.

Changing risk profile

The trend towards prefabrication and modular building will have big implications for the construction industry's risk profile.

Significantly, it has the potential to de-risk the onsite construction process, transferring activities to a safer and more controlled factory

environment. Construction sites can be hazardous places to work, but with prefabrication the time spent onsite can be greatly reduced, as can the number of workers.

However, much of the risk will shift to manufacturers, while prefabrication could increase the risk of supply chain disruption. A fire or flood at a factory, or damage to modules during transportation, could result in long delays onsite. Modular buildings also typically require more heavy lifting. With more cranes comes a higher wind exposure, which could mean a greater number of days lost onsite to bad weather.

Fire is another concern. The design, installation and testing issues seen with some types of external cladding are a red flag for potential risks of modern construction. Where modules are finished or assembled onsite, there is a risk that fire protection could be compromised, while the potential for voids inside prefabricated walls could enable fire to spread.

Design risk

Prefabrication and modular construction could increase design risk. New designs and construction techniques have caused problems in the past, especially where developments have been rushed to meet demand for more homes.

The post-war boom in non-traditional building and the government-subsidised prefabricated homes of the 1960s and 1970s, for example, experienced well-documented failings and defects.

Design flaws in prefabricated buildings would likely pose a systemic problem that could affect far more buildings than traditional bespoke developments.

Recent experience has also shown durability issues with new modular systems. Buildings initially perform well, but later suffer issues with connections between modules and weather-proofing. The Oxley Woods prefabricated development in Milton Keynes, for example, won awards for innovation, but later experienced a catalogue of problems related to water ingress and damp.

Insurers will want to see that systems have been properly tested against field conditions, such as environmental testing, computer modelling and full-scale tests, including fire. Underwriters will want comfort that systems meet the intent and requirements of building regulations, and not simply particular aspects of the approved documents. In particular, insurers will want to understand how access will be gained to remedy defects and whether voids introduced into modules, or onsite activities and DIY, could negatively impact fire performance.

Quality control is likely to be an important factor in the success of new modular builds. Robust control processes in a factory environment could raise quality standards, but rigorous monitoring and verification of materials, workmanship and testing in the supply chain will be critical. Experienced management could also be essential, especially where skilled onsite trades are replaced by semi- or unskilled factory workers. The development of detailed process specifications for the installation of modular elements on site, as well as the training and monitoring of the workforce carrying out these activities, will be critical.

Insurance

The growing use of non-traditional construction methods like modular buildings will have important implications for insurance. Policy wordings will need to reflect changes in risks, such as the increase in offsite construction and transport exposures, to ensure that insurance responds. Risk engineering will also need to adapt to offsite construction and the proto-type nature of new materials and methods.

Andy Kane is Portfolio Manager, Construction at QBE European Operations
www.qbeeurope.com

New dimensions

Working from home was BAU for many, long before COVID-19, but, as Deborah O'Riordan writes, the unprecedented scale of reaction and government intervention in this pandemic creates an unprecedented human challenge

While many employers have embraced the benefits of agile working, few have experienced an entirely remote workforce. The same is true for most employees too who may be used to short stints at home but are wholly unaccustomed to extended, unbroken periods of remote working.

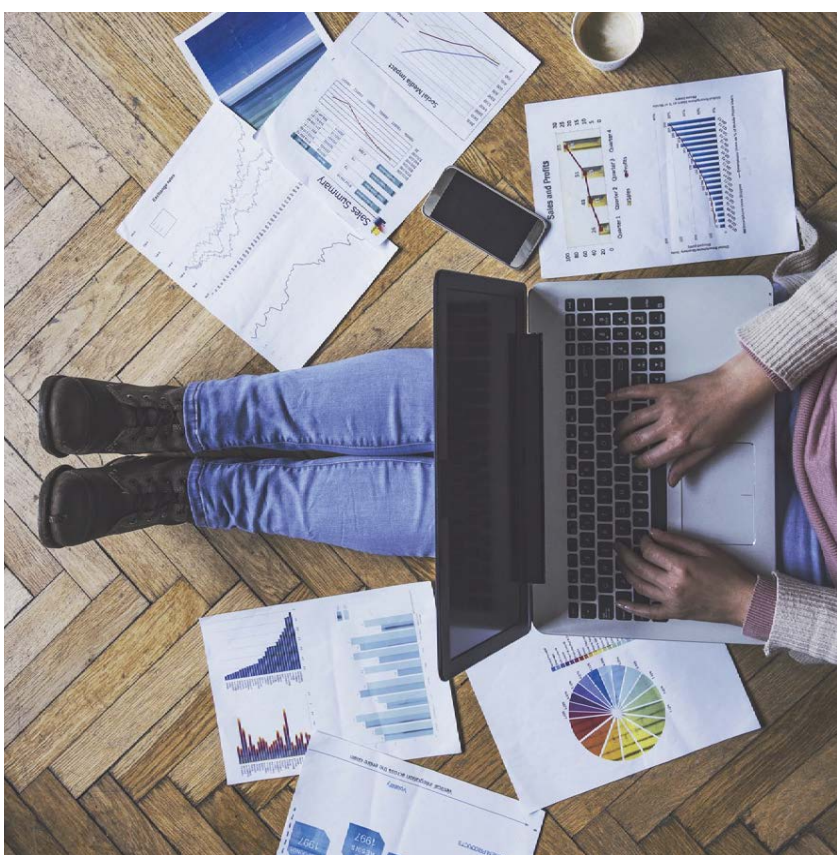
COVID-19 is changing the situation for many companies, forcing workers into potentially prolonged periods of isolation. The potential impact on mental health is significant, but there are steps that both employers and employees can take to minimise its effects.

EMPL OYERS

Regular communication is key

Employees perform better when they are engaged and motivated. Places of work tend to be stimulating, with lots going on. When working remotely, communication can often feel less frequent and the home environment less invigorating. It is advisable therefore for employers to increase formal and informal communication.

Communication methods should be mixed up – a video or telephone call is more interactive than an email and helps break up the monotony of working from an inbox. Video calls also allow the opportunity for face to face interaction and enable teams to talk collectively. Using instant messaging platforms can help change the tone and tempo of responses and may be a more favoured communication medium for some.



Teamwork keeps people engaged

It's worth considering whether some tasks should be completed as a team instead of individually. Collective team participation helps team cohesion and keeps people engaged. The benefits of teams working collectively will likely outweigh any short-term negative effects of increased task completion time. Just because employees are working from home does not mean they have to feel like lone workers.

Technology and IT equipment

Employers must consider that IT equipment may limit productivity in some way eg. home broadband may be slower and laptops with small screens can be a challenge for those used to working on large or multiple monitors.

Mental health and well-being take priority

For some employees remote working might be more challenging. During a period of transition, it is good practice to check in with employees regularly to see how they are feeling

and coping. For some companies this may already be part of their culture and working practice but for others, it may require a change in approach which may initially be met with scepticism and suspicion by employees.

Employers should remind employees of mental health services available to them and, if possible, re-run any mental health, well-being and resilience training courses. It is also important to remind employees that it's acceptable and encouraged to report problems, this should be reinforced regularly by people leaders. Some Employee Assistance Programmes (EAPs) offer proactive counselling, should it be required.

EMPLOYEES

When used to the hustle and bustle of the work environment, extended remote working may come as a real shock to the system for employees, particularly those who live somewhat isolated lives outside of the workplace already. It is critical that workers continue to feel connected to colleagues and exercise the right discipline at home. They should:

Helplines

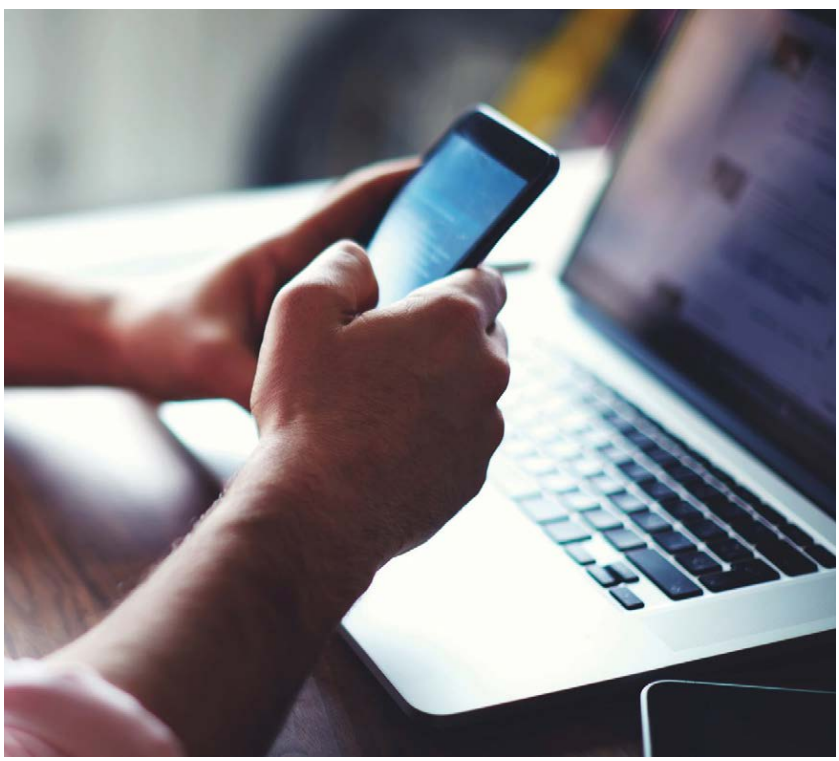
If employees are struggling at home and feel they cannot tell their line manager or colleagues, there are many confidential and free helplines out there that can help, including

Mind – https://www.mind.org.uk/helplines/

Samaritans – https://www.samaritans.org/how-we-can-help/contact-samaritan/

Stick to normal working hours

Without the structure of commuting to and from the workplace, the working day can creep, with no clear 'clocking off' point at the end of the day. The result is employees never really switch off and risk burning out quickly.



"Collective team participation helps team cohesion and keeps people engaged"

Take regular breaks

Employees need to be disciplined also around taking breaks, whether it is as simple as going to get a drink or stepping outside to get some fresh air. According to government guidelines, even those who are self-isolating should take regular exercise outside, just ensuring they avoid crowded places and keep a good distance between themselves and others.

Regular breaks are particularly important from an ergonomic perspective also. Typically, home desks are less adaptable than office desks and unlikely to have been assessed by postural experts. Movement and light stretching every 30 minutes is recommended.

Eat healthily

Maintain a healthy diet to avoid the sluggish feeling of being at home. Constant grazing can often be a downside of remote working. If it is a difficult habit to break, at least try to keep snacks healthy.

Keep in touch

One of the ways to combat loneliness during prolonged isolation is to set up regular video calls with teammates. If employees are struggling at home either mentally or physically, they should let their colleagues, line manager or mental health first aider know at the earliest opportunity.

Deborah O'Riordan is Practice Leader, Risk Solutions at QBE European Operations
www.qbeeurope.com

Delegated authority schemes spotlight

Deborah Ritchie speaks to John Dawe about the benefits of a scheme, what the journey looks like, how RSA helps partners maintain compliance, and much more

For the benefit of brokers who may not be clear, what exactly is a scheme?
A scheme is very much a relationship between a customer with a unique group of characteristics, a broker and also an insurer such as RSA. We always start with a focus on the customer, truly understanding who they are and what their insurance needs are. If a broker is able to understand those needs, it gives them a unique opportunity to be able to create solutions to meet those customer needs. They can deliver those using their own brands and also be in control of the whole customer experience.

The role of an insurer like RSA is to be able to facilitate and enable the broker to be able to write risks on behalf of those customers we delegate and extend our authority to them. So, they can write those risks supported by an underwriting guideline and framework. We also work with that broker to build a bespoke product specifically for that customer group.

What makes a successful scheme?
A successful scheme is one that's underpinned by a long-standing partnership between an insurer and a broker. Schemes are not quick wins. They take time and collaboration to create, launch and then grow into a successful partnership. What works really well is when you can take the expertise and the experience and resource of an insurer and combine that with the knowledge that a broker brings about really understanding a particular customer group and what makes a customer tick. When you combine that together you're able to really extract value out of a scheme, make it profitable and make it grow.

Can brokers easily transfer an existing scheme to RSA?
Absolutely. We've got a really broad appetite and a very open mind and we welcome brokers with existing schemes to come to us and discuss how we can take their schemes to the next level and explore opportunities for new ideas that brokers may have. Come and reach out to us. We'll review those opportunities and can make a really quick decision as to whether they're for us.

If they are, then we have a tried, tested and established process for transferring those schemes over to RSA, supported by a dedicated implementation manager, which takes away a lot of the hassle to create a smooth migration process. It also gives us the opportunity to start a conversation with brokers about some of the exciting ways in which we could take their schemes to the next level, such as looking at product enhancements we can put in place or different ways we can distribute products for greater customer reach.

What tangible benefits can brokers expect from a scheme?
A scheme is a really great opportunity for brokers to be able to grow their business – particularly if they're able to identify a customer group with a unique set of characteristics that is unserved or untapped in the market. Many of those customers won't be able to get these types of covers in the open market from standard SME products. The creation of a specific product to meet their needs through a scheme gives the broker a real unique selling point. Equally, schemes customers have very high retention rates compared with non-schemes customers. They're really sticky, which means that brokers are able to develop real long-term, deep-rooted relationships with those customers.

"We've got a really broad appetite and a very open mind and we welcome brokers with existing schemes to come to us and discuss how we can take their schemes to the next level and explore opportunities for new ideas that brokers may have. Come and reach out to us."

This also gives them greater opportunities for increased revenue – especially in areas such as cross sell and up sell.

As a scheme partner, what does RSA offer in particular?

At RSA, we are absolutely dedicated to schemes. We've got a specific team that only deals with schemes and delegated authority. So, we're real experts in this area. We've got an open mind and a broad appetite for a whole range of opportunities. We make available partnership managers who will be with the broker in order to extract the full value out of the scheme over the long term.

We also make available experts from within RSA across compliance, claims and underwriting. We're really keen to find ways in which we can help brokers and their businesses to grow. We look at all of the data that we built over our history, as well as buying additional data to apply to a broker's business to help us understand how we can extract more value out of their schemes. That's in addition to being able to provide risk management consulting and training.

What does RSA need from a broker to explore a scheme's opportunity?

When a broker approaches us with a new opportunity, the first thing we'll do is to try to understand the broker's business – to really get them and get what's important to them. Then, the broker can share with us their knowledge of the targeted customer segmentation where they feel there's a real opportunity to create a thriving scheme.

The brokers that we like working with are those with a real appetite and passion for schemes, and especially those that are looking to work with us over the long term. The more that a broker can share with us, the more we're able to create a profitable solution that will grow over the long term.

What are RSA's risk sweet spots?

We approach every opportunity with an open mind. There's no such thing as a typical scheme, but in the main, we look for customers from UK-domiciled medium-sized businesses. We also look to support schemes that have premium of around £250,000 plus or at least have a plan to be able to grow a scheme to that scale. From a risk perspective, we like low to medium hazard risks, but we're really excited to be able to support our customers and their businesses with risk consulting and risk management support.

A good example of where we're looking at the moment is the untapped potential of the artisan space, including gin distilleries, micro-breweries, costume jewellers and horticultural nurseries. Those types of trades are particularly exciting at the moment.

What does a typical scheme journey look like on a practical level ?

We break the scheme journey into four simple phases. The first phase is all about getting to know you. We're really interested in your knowledge as a broker of the target customers, understanding what makes those customers tick and why you think that we can create a thriving scheme together. We'll review whether it's within appetite, whether it's scalable and whether we think there's value for both RSA and also for the broker. If we achieve that then we get to the really exciting bit. We can get together and start to think about the proposition and the product that we're going to create and take to market together.

The second phase is all about developing our partnership and this is really important because we

"The brokers that we like working with are those with a real appetite and passion for schemes, and especially those that are looking to work with us over the long term. The more that a broker can share with us, the more we're able to create a profitable solution that will grow over the long term."

know we're going to have a long-term partnership together so it's really important that we understand your business and how you operate. We'll connect our respective experts with experts at the broker who speak the same language, and we'll establish how we'll work together going forward - so it's really efficient and effective.

The third phase is all about preparing to go live and this is where we pull together a project plan led by a specialist delegated authority project manager who's got a wealth of experience in a tried and tested process for ensuring we've thought of everything. That's really important because it gives a broker peace of mind that everything is thought of and that it will be seamless and efficient and effective and we'll keep the broker updated on timescales and delivery at every step of the way.

Then, once we've gone live, the final phase is what we refer to as a deepening and strengthening of our partnership. We jointly set up regular contact between a broker and an allocated partnership manager to ensure the scheme is operating as we intend it to. We'll find ways in which we can really add value to the proposition and ensure that we're always working with the broker to give them a competitive edge.

"RSA really understand what the regulator expects when it comes to transacting business to customers through a delegated authority chain. And because we know what the regulator requires, we can protect our mutual customers and we know what we need to do to protect our scheme brokers as well."

What support can a broker expect from a dedicated partnership manager?

A broker will be provided with a partnership manager throughout the lifetime of a scheme and they'll be responsible for the day-to-day operation and running of that scheme. They're also responsible for making sure the scheme fulfils its potential and will work with the broker in a relationship to achieve that. The partnership manager will find ways to fine-tune the proposition, identifying further opportunities to give the broker a competitive edge. They also take care of any troubleshooting, making sure that issues are dealt with so they don't get in the way of the broker being able to trade.

They will also connect a broker with various experts within RSA including our claims, underwriting and compliance professionals. There are also opportunities for a partnership manager to understand what the broker's business needs and find ways in which RSA can add value through training or finding ways in which we can use data to create insight to help with the ongoing profitability and performance of the scheme.

How does RSA help brokers support compliance?

Because RSA has a team that is dedicated to delegated authority business, we really understand what the regulator expects when it comes to transacting business to customers through a delegated authority chain. What that means is that we know what the regulator requires and that means we can protect our mutual customers and we know what we need to do to protect our scheme brokers as well.

The types of activity that we'll undertake are regular product reviews to ensure that our products are working in the best interests of customers. We'll undertake regular reviews of conduct MI to ensure that value is being created in the products that we sell to our customers. What that means is that within our relationship it's really important that our brokers are able to provide the right level of really good quality conduct MI for us to review collectively together, that they take their responsibilities really seriously in terms of the activities that they undertake, such as selling of the product and making sure that is in the best interests of the customer and generally ensuring that brokers really have a culture of putting customers at the heart of everything that they do.

John Dawe is Partnership Director for Delegated Business at RSA

For more information about RSA's schemes, speak to your local RSA representative or visit the delegated page at rsabroker.com

Interviewed by Deborah Ritchie

NATIONAL INSURANCE AWARDS 2020

WINNERS' REVIEW

5 MARCH 2020, THE WALDORF HILTON, LONDON

Brought to you by

Insurance Today

In partnership with

CIR
CONTINUITY INSURANCE & RISK

Supported by

Chartered Insurance Institute

nationalinsuranceawards.co.uk

Innovative Product Award
WINNER: Charles Taylor Insuretech and The London Market Group

Commercial Lines Broker of the Year
WINNER: Romero Insurance Brokers

Commercial Lines Insurer of the Year
WINNER: Direct Line for Business

Commercial Lines Insurer Claims Team of the Year
WINNER: Direct Commercial

Personal Lines Broker of the Year
WINNER: Vizion Insurance Brokers

Personal Lines Insurer of the Year
WINNER: Voyager Insurance Services

Initiative of the Year
WINNER: YPO in partnership with ESPO and NEPO

Claims Initiative of the Year
WINNER: Sedgwick International UK with L&G Geobear

NATIONAL INSURANCE AWARDS 2020

Schemes Broker of the Year
WINNER: Stanmore Insurance Brokers

Lloyd's and the London Market Award
WINNER: Charles Taylor Insuretech and The London Market Group

InsurTech Award – AI/ML and Modelling
WINNER: Kovrr

InsurTech Award – Technology & Infrastructure
WINNER: Lightfoot

Communications Team of the Year
WINNER: AXIS Capital

Growth Company of the Year
WINNER: The Churchill Business Team in Direct Line Group

Insurance Recruiter of the Year
WINNER: Idex Consulting

Insurance Law Firm of the Year
WINNER: Forbes Solicitors

Digital Insurance Award
WINNER: International UK & Typhoon 8

Inclusion and Diversity Award – External Programme
WINNER: Chartered Insurance Institute

Inclusion and Diversity Award – Internal Programme
WINNER: Travelers Europe

ESG Award
WINNER: Texel Finance

NATIONAL INSURANCE AWARDS 2020

Institute of Risk Management

The International Certificate in Enterprise Risk Management

Enterprise Risk Management (ERM) is at the heart of all our efforts to tackle the current pandemic and the Director-General of the World Health Organisation recently called for an enterprise-wide approach.

Have you got the expertise you need?

The International Certificate in ERM is the ideal qualification for anyone looking for a solid foundation in the theory and practice of effective risk management. Get the skills you need now to tackle the challenges of risk management and learn how to manage extraordinary crises in the future.

Working together through uncertainty

What our students say

Carla Knight IRMCert
Risk Management Specialist, Exxaro Solutions, South Africa
"IRM qualifications are an excellent way to ensure that you stay relevant and on top of the changing risk management field. It has taught me so many things especially in the areas where I do not see myself as an expert."

Byron Tidswell IRMCert
General Manager Risk, Assurance and Audit, V/Line, Australia
"The International Certificate in ERM provided a really practical and useful framework to think about operational and enterprise risk. It has been invaluable to me in continuing to build performing risk management functions."

To find out more about the IRM's International Certificate visit:

www.theirm.org/cir-erm

irm
Developing risk professionals

CIR | Risk Management

AWARDS 2020

THE CATEGORIES

The 11th annual Risk Management Awards

The pinnacle of achievement in risk management

cirmagazine.com/riskmanagementawards

Sponsored by

Regus workplace recovery

Headline Partner

irm
Developing risk professionals

Supported by

airmic

ALARM
embrace risk

London Marriott Hotel, Grosvenor Square

Categories 2020

1. Risk Manager of the Year
This award is the hallmark of outstanding performance by the risk management professional who has accomplished most in the past 12 months in reinforcing their organisation's risk management framework, inspiring their team and offering creative thinking to the risk management community as a whole. Risk professionals in organisations ranging from FTSE 100 blue chips to small and medium-sized enterprises are all potential contenders for this award.

2. Risk Management Champion Award
This award will be presented to the individual deemed to have contributed most to the world of risk management in the opinion of the judges.

3. Newcomer of the Year
This award will be granted to the risk management professional within the last five years. They may be from another discipline or have just started their career. Entries must be able to demonstrate the impact this individual has had upon risk management within their organisation or the sector.

4. Risk Management Team of the Year
This award will mark the best collective achievement in risk mitigation teamwork within an organisation. Contenders will be able to demonstrate that ideas and efforts that individual team members have contributed towards an overall risk initiative. Entries will be accepted from teams of businesses of all size – from SMEs to major multinationals.

RISK MANAGEMENT PRACTICE

5. Cyber Security Initiative of the Year
For response planning and penetration testing against an ever-growing challenge in keeping one step ahead of hackers and online criminals who are ready to exploit any weak link within IT systems, this award is for the organisation that has devised the most innovative and effective methods of preventing cyber crime and protecting their organisation's assets.

6. Operational Risk Initiative of the Year
For teams, individuals, consultancies or companies, this category recognises an initiative that has created increased security within financial operations. Both innovation and original thinking will be rewarded. The judges of this category will be drawn from experts, and we acknowledge the potentially sensitive nature of submissions, so beyond the normal NDA we will also allow descriptive rather than technical nominations.

7. Risk Management Programme of the Year
This award is designed to recognise a sustained single programme with risk

Categories 2020

management at its heart. This might be to reduce accidents within its fleet, manage incidents on a construction project or mitigate exposure to risk in financial transactions. If there is one particular aim of this programme and it can be demonstrated to have achieved results then it is eligible. The judges will seek evidence of success against a clearly defined target.

8. Cross-Border Risk Management Award

This award will be presented to the organisation that can demonstrate how it has built a risk management function capable of operating across multiple business and legal jurisdictions that are geographically diverse (across international boundaries and cultures), including from within the UK. Entries should outline the organisation's risk management programme, the development, scope and achievements of its team(s) and the way in which it communicates the risk message to the wider company – and how all of these align with local conditions as well as overall organisational goals.

9. Major Capital Projects Award

Robust risk management is essential in ensuring that major capital projects are delivered on time and to budget. With many different parties involved, co-ordination is also a major element. This award recognises a project that has successfully met these criteria and can be considered a major project in its scope.

10. Public Sector Risk Management Award

This category seeks to reward the team that has tackled the inherent risks of operating within a public sector environment. The winning team will be able to demonstrate best practice from which all organisations can learn. In a period where many in this segment have suffered major cuts to budgets, this award is especially well deserved.

11. ERM Strategy of the Year

This award will be presented to the company which has best demonstrated the implementation of an enterprise risk management (ERM) programme, which includes the integration of ERM into the culture and operations of the business, to solve real-world business problems.

PRODUCTS AND SERVICES

12. Risk Management Product of the Year

This category focuses on products and solutions that have delivered real value to organisations and which have possibly spawned imitators – which is the true proof of a ground-breaking innovation. Entrants must be a concept that can be implemented or a technological solution.

13. Risk Management Specialist Company of the Year

This award will be presented to the company that is dedicated to providing effective risk management solutions to its clients. Entries should detail products, services or projects undertaken and how success was achieved. Judges will award innovation and quality as well as customer service and satisfaction.

14. Cyber Security Product of the Year

This award will be presented to the company whose product most successfully demonstrates their advanced skillset in dealing with the growing threat of cyber risk. Successful submissions will demonstrate the providers understanding of the diversity of this risk, and scalability to respond to the threat as it evolves. Entries may include a demo (of no more than 5 minutes).

GENERAL CATEGORIES

15. Best Use of Technology in Risk Management

This award will reflect the ability of an organisation to proactively use technology for delivering recognisable benefits in its management of risk, whether from a vendor or developed in-house. The category is ONLY for technological solutions, and evidence of implementation will be given extra consideration.

16. Risk Management Innovation of the Year

Judges are looking for an innovation that has been initiated for the first time during the 18 months before the entry deadline, and which has the potential to

Categories 2020

change the way in which a segment of risk management can be conducted. This could be a product or a process, but will need to show innovation and original thought.

17. ESG Risks Initiative of the Year

This award will be given to the organisation that has made significant progress in assessing environmental, social and governance risks to organisations. The judges will want to see strategy, long-term vision and evidence of success. Please note, this is a risk award, and we are looking for initiatives to assess, reduce and protect from risks, rather than activities may well be worthy but are not directly associated to the practice of risk management.

18. Political Risk Award

The category for outstanding provision of political risk management expertise. Aimed at honouring the provider of political risk management, and the implementation of such strategies, judges will look for details of the identified risks, and information related to the strategies undertaken to mitigate them.

19. Diversity Award

This award will be presented to the organisation that can demonstrate a commitment to diversity in its risk management activities. Entries should present the organisation's policy towards diversity in the workplace and demonstrate how this policy is implemented practically in the way that risk management staff are recruited, trained and promoted within the organisation. Entries should demonstrate how the organisation supports and promotes diversity in the context of managing risk.

20. International Risk Management Award

This award will be presented to the organisation that can demonstrate that it has built risk management into the very heart of its operations – encompassing the full scope of enterprise risks. Entries should outline the organisation's risk management programme, the development, scope and achievements of its team(s) and the way in which it communicates the risk message to the wider company – and how all of these align with local conditions. This category is open to companies without a UK office.

21. Public Safety Award

This award will be presented to the organisation that has demonstrated the most success in developing a product or innovation of any kind that has as its sole focus the safety of the public. Examples may include innovative reporting or warning systems, safety solutions for crowded places or security in the built environment, for instance.

CIR Risk Management AWARDS 2020

2019 Winners

Diversity Award
Winner: Control Risks

Risk Management Innovation of the Year - sponsored by Regus Workplace Recovery
Winner: Equifax
Highly commended: Web Shield

Best Use of Technology in Risk Management
Winner: Arcadis Consulting

Best Use of Technology in Risk Management (partnership) - sponsored by Blackberry
Winner: Network Rail and SharpCloud

Cyber Security Product of the Year
Winner: FM Global
Highly commended: Code42

Cyber Security Initiative of the Year
Winner: Blackfoot Cybersecurity

Risk Management Specialist Company of the Year
Winner: Aviva Risk Management Solutions

Risk Management Product of the Year
Winner: Acin

Risk Management Product of the Year (Service)
Winner: International SOS

Public Safety Award
Winner: Ecclesiastical

International Risk Management Award (Business)
Winner: Abdul Latif Jameel Co.

International Risk Management Award (Public Sector)
Winner: Dubai Electricity and Water Authority

ERM Strategy of the Year
Winner: LyondellBasell
Highly commended: BT

Public Sector Risk Management Award
Winner: Northern Ireland Water and Turner & Townsend

Major Capital Projects Award
Winner: A14 Integrated Delivery Team

Risk Management Programme of the Year
Winner: Southern Water

Operational Risk Initiative of the Year
Winner: Aviva

Newcomer of the Year - sponsored by Aon
Winner: Alex Todorova, Mott MacDonald

Risk Management Team of the Year
Winner: Nationwide Building Society

Risk Manager of the Year - sponsored by Regus Workplace Recovery
Winner: Simon Cory, Nationwide Building Society

Industry views

There is much debate about the extent to which we have entered a true hard market. Evidence from our own members strongly indicates that price rises in some classes have indeed been significant and renewals have been challenging.

However, the current conditions are different from previous hard markets which were mostly about price. Today we are seeing a broader range of factors, including a negative impact on deductibles and capacity, the late timing of presentation of renewal terms, and in some cases the complete withdrawal from certain classes of cover or sectors. We are also starting to see a negative impact on claims.The biggest challenge for our members has been the speed of change and lack of communication and consultation. Decision-making has become centralised, with little inclusion of the end client, to the extent that it has affected the timing of renewals. And while in many cases price rises appear justified, in other instances pricing feels aggressive and opportunistic.

We have suggested three key areas where the market can better support policyholders: improve pricing communication; start the renewals process earlier; and reward strong risk management. For risk professionals, this is the time to be proactive and take the lead. Preparation has never been more important. Policyholders should understand and be able to articulate their risk appetite with absolutely clarity. Renewal submissions must be first-class, tailored to business and sector and highlighting risk management achievements and plans. Communication with the C-suite is also vital. Regular constructive discussions – possibly even inviting the CFO to a renewal meeting – help to manage expectations so there are no nasty surprises.

These are challenging conditions for all, but there is a greater opportunity here. The prolonged soft market has contributed to insurance being seen as an increasingly commoditised purchase. The harsh market is moving it back up the boardroom agenda. This can used to remind organisations of the value of a professionally constructed insurance programme. That is a win for all.

John Ludlow is chief executive officer of Airmic

In association with airmic

March was going to be a big month for us at the CII. The FCA was going to publish its discussion paper, Transforming Culture in Financial Services. We had led an insurance working group, which had carefully prepared one of its chapters. The FCA's paper, like everything else, was swamped by the global disaster unfolding around COVID-19. But I'm still glad we did that work. It taught me some useful lessons about where the insurance sector should be heading – lessons that have been put into even more stark relief in recent weeks.

The key controversy around COVID-19 and insurance has been around the scope of business interruption insurance, with many businesses angry that their cover did not give them more protection from the massive economic impact of the virus. This kind of controversy is not new. We have seen similar gaps between expectations and reality with cyber insurance and before that, with different forms of liability insurance.

Given the limits to which our clients can bring themselves to focus on the finer points of their insurance policies, it is not credible for us, as a profession, to tackle the problem through policy literature alone. We need to start by thinking about all the risks our clients face, not just the insurable risks. For example, one leading broker has adopted this new approach simply by rethinking is annual meetings with corporate clients. It had always put renewal of cover at the top of the agenda, and uninsured risks at the bottom. It has now switched this around, talking about uninsured risks first, along with how clients plan to manage these risks, and renewal of cover at the end. This means clients come out of the meeting with a much greater understanding of the risks they face and the part insurance plays in managing those risks. It gives clients the ability to understand the limitations of their cover without feeling cheated later on.

When life begins to return to some form of normality, this lesson – about looking at the whole customer and prioritising their biggest and most difficult risks – is one our profession must not forget.

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

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

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

We cannot avoid talking about the pandemic currently affecting the global business environment. It is, as Prime Minister Boris Johnson said in one of his many recent briefings, "the worst global health crisis in a generation".

The director-general of the World Health Organisation, Dr Tedros Adhanom Ghebreyesus recently called for an enterprise-wide approach to battling the pandemic – one which places enterprise risk management at the centre of the crisis. We will soon see how our education, training and professional development has equipped us, and our organisations, to tackle this major risk.

The true impact on businesses will not be able to be gauged for some time, although we can see many businesses – from major airlines to local small-to-medium sized enterprises – already voicing their concerns about sustainability going forward and requesting assistance and guidance from the government.

Public health measures in the UK are currently focusing on delay; on slowing down the spread of the virus and reducing the numbers affected. The aim is to lower the peak impact and push it away from the winter season, initially by detecting and isolating early cases.

"Some less risk mature organisations will be in uncharted territory which will – inevitably – lead to some businesses folding"

More severe measures may be put into place, for example reducing public gatherings, closing schools and restricting public transport, should it be deemed by the government to be necessary and cost-effective, although such measures would incur significant economic and other costs. As risk professionals, we are skilled at framing and understanding these difficult policy choices.

Preparedness is key, effective risk management and business continuity plans now kicking into place will play a pivotal role. Some less risk mature organisations will be in uncharted territory which will – inevitably – lead to some businesses folding.

A core principle of risk management is to learn from experience and improve; there will be lessons from the experiences of dealing with the challenges of COVID-19 which will result in improved resilience and better risk management in the future.

Global supply chains are being affected. On this topic, some readers will be interested to know that the IRM recently launched its new Supply Chain Risk Management Certificate in conjunction with the Supply Chain Risk Management Consortium). Founder of the Consortium and risk expert, Greg Schlegel says: "Most businesses do not embrace or embark on a strategic risk journey UNTIL they experience a risk event. If they do it's all hands on deck 24/7, in an attempt to survive the event. If they do survive the event a lot of companies will go back to business as usual. Many companies do not survive a moderate-severe global risk event like the COVID-19 virus."

In combatting this, one of the challenges for risk managers will be to ensure there is a balanced, proportionate and common sense approach.

Iain Wright is chairman of the Institute of Risk Management

In association with irm

The importance of adaptation financing

The benefits of adaptation projects are usually significant, but development is hindered. To combat this, David Masters says it's vital that the resilience benefits of such investments be quantified in financial terms

Exacerbated by climate change, the frequency and severity of extreme weather events are increasing. As such, the need for adaptation projects – those that strengthen the resilience of buildings, critical infrastructure and communities against these climate-related risks – has garnered increasing attention.

Adaptation projects often generate returns at a multiple of their cost, but the sheer size of the adaptation financing gap, the enormity and complexity of such projects, and constrained public finances are all hindering development.

While increased engagement from the private sector would ultimately lessen the financial burden on public sector entities, private investors face their own set of risks and difficulties in assessing the long-term returns associated with investing in adaptation projects. But if the benefits of such investments can be quantified in financial terms, as well as environmental, we believe that a strategic collaboration between public and private sector financing could become the most likely path to success. For the insurance sector as a whole, adaptation projects provide opportunities across both sides of the balance sheet.

Investment in adaptation can offer a certain level of cost-effective protection against physical damage caused by extreme weather – something we define as a 'resilience benefit'. Indeed, investment in improving early warning systems against natural disasters can generate returns of almost 10 times their cost.

The consequent economic disruption from severe weather events can often extend beyond the affected region through global supply chains. The 2011 floods in Thailand, for example, impacted global technology and car production because the manufacture of key parts was concentrated in the flooded area. Consequently, over 50% of insured losses, totalling over £12bn, stemmed from business interruption claims.

Areas that invest in adequately protecting themselves against extreme weather events may also see considerable secondary financial benefits as improved resilience may promote economic development. Between 2017 and 2019, weather-related insurance pay-outs were the equivalent of £222bn globally – the highest 24-month figure on record. Reduced natural catastrophe risk, therefore, could support decreased insurance costs, bringing yet further indirect financial benefit.

The adaptation finance gap

Yet despite a general acknowledgement of the urgent need for climate adaptation projects among public authorities, including in countries such as Bangladesh, Indonesia, the Philippines, and densely populated areas of the US, such as Boston and New York, implementation is slow.

While authorities may be under scrutiny if they fail to develop the adaptation infrastructure necessary to protect communities from climate-related damage and disruption, the challenge of effective adaptation design that delivers the expected benefits, compounded by potential negative social impacts to communities, may deter authorities from pursuing adaptation projects. The often slow implementation is, at least partially, due to the high costs involved – and in times of strained public finance, these projects are unlikely to be high priority.

In fact, to meet resilience needs, current adaptation financing needs to increase substantially. In 2018, about 6% – or £27bn – of total global climate change investments focused on adaptation projects. The United Nations Environment Programme, however, estimates that this investment will need to increase by 4x-9x by 2030 to meet resilience needs, highlighting a significant gap in adaptation finance which public entities cannot achieve alone.

Against this backdrop, we believe that there is a need to attract private finance support in this area – especially given the interest in climate finance opportunities among the investor community. Private investment in climate change adaptation, however, is currently around a modest £404m, with significant room for growth.

In order to engage the private sector and bridge the current climate adaptation financing gap, it is vital that the resilience benefit of such investments is quantified in financial terms. Despite the difficulties in doing so, private investors must be able to justify the allocation of capital to projects whose benefits may only emerge many years in the future.

One way to calculate the resilience benefit of an adaptation project could be to estimate the reduction in expected damages that the infrastructure funded by the green bond is designed to achieve over the targeted period. If the cost benefits are clearly outlined in this way, private investors could be more inclined to engage and seek opportunities, such as transfer of risk to the capital markets in the form of insurance, catastrophe bonds, or other derivative instruments, as well as the support of contingent financing from multilateral institutions and governments. Meanwhile, constrained public finance would receive the boost needed to achieve widespread resilience against the ever-increasing effects of climate change.

David Masters is a director at S&P Global Ratings

ClearView Continuity
Astral House
Granville Way
Bicester
Oxfordshire
OX26 4JT

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

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

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

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

ClearView – we make the complicated simple.

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

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

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

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

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

JCAD's software is wholly "off the shelf " which enables time efficient implementations, low cost systems and simpler training. Additionally, by offering a best practice approach to risk and compliance management we can focus on the development of new functionality that is then shared across our entire client base. JCAD are an ISO9001 accredited supplier and our hosting partners are accredited to ISO27001. Our risk management software will align to such standards as ISO3100, COSO and guidance from the OGC.

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.

---

ventiv TECHNOLOGY

Ventiv Technology
30 – 40 Eastcheap
London EC3M 1HD

Contact: Steve Cloutman

Tel: +44 (0) 7971 505433
Steve.cloutman@ventivtech.com
www.ventivtech.com
LinkedIn: www.ventivtech.com/linkedin
Twitter: @ventivtech

Ventiv Integrated Risk Management (IRM)
Whether you're managing risk, safety or insurance programs, your job is more challenging than ever. More data. Increased business complexity. Greater security risks. Heightened expectations. Less time to respond, and with fewer resources. You need a technology solution that meets today's needs while demonstrating the ability to meet tomorrow's challenges, too. The answer is Ventiv IRM.

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

Fully embedded and integrated into Ventiv IRM, Ventiv's analytics, reporting and data discovery is the market's newest and technologically most current offering. Ventiv is the only RMIS provider offering cutting-edge **Automated Predictive Analytics** as an embedded and integrated component of our solution. All this empowers you to deliver data-driven decisions that generate optimal outcomes like reducing total cost of risk.

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

RISK MANAGEMENT SOFTWARE SOLUTIONS

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.

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.

BIBA TWENTY21

BIBA MANCHESTER CENTRAL | MAY 12/13

Save the date

Europe's largest insurance broking event will return on May 12 & 13, 2021.

We look forward to seeing you back in Manchester next year

The BIBA team