

**The interview**

The lowdown on greenwash  
with Clare Hobby

**Book review**

Catastrophe and Systemic Change: Learning from  
the Grenfell Tower Fire and Other Disasters

**Executive summary**

Highlights from the new  
ClimateWise report

cirmagazine.com

July-August 2021

# CIR

CONTINUITY INSURANCE & RISK

➤ **Building Safety Bill** *The long-awaited Bill will bring about a number of major changes that insurers need to be aware of*

➤ **Training risk champions** *The role of risk champions in establishing an effective ERM structure and culture*

➤ **Podcast highlights** *Cyber exposures and underwriting in financial institutions, with sector experts at Tokio Marine HCC*



## The chips are down

➤ Post-pandemic supply chain risk management

➤ View: "The first three months of lockdown accelerated the digitisation of the insurance world by five years"





## CYBER INSURANCE

Cyber risks are happening more frequently and the cost of cyber incidents is rising.

At AXIS, we offer more than insurance. The AXIS cyber team will help businesses unlock the secrets to being cyber resilient.



### PREPARE



AXIS offers services and tools to help prepare businesses and make them more cyber resilient.

### PROTECT



AXIS Cyber Insurance is built to protect businesses in today's environment and works alongside businesses' security tactics to protect them.

### RESPOND



AXIS can support businesses' recovery as they respond to a cyber incident, beyond just claims.

Visit [axiscapital.com](https://axiscapital.com)

Copyright © 2021 AXIS Insurance. AXIS Managing Agency Ltd ("AMAL") is registered in England (Company Number 08702952) with a registered office at 52 Lime Street, London, EC3M 7AF. AMAL is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority (Firm Reference Number 754962). AMAL manages Syndicate 1686 and is additionally subject to the supervision of the Society of Lloyd's. AXIS Specialty Europe SE ("ASE") is registered in Ireland (Registration Number 353402 SE) at Mount Herbert Court, 34 Upper Mount Street, Dublin 2, Ireland. ASE is authorised by the Central Bank of Ireland and subject to limited regulation by the UK Financial Conduct Authority. Our address is 52 Lime Street, London EC3M 7AF. Underwritten in the US by AXIS Insurance Company (NAIC # 37273), an Illinois property and casualty insurer, licensed in all 50 states of the United States and the District of Columbia, with offices at 111 South Wacker Drive Suite 3500 Chicago, IL 60606.

## Comment

Severe flooding across Germany and other areas of Western Europe this month brought enormous human suffering to the region, with reports of over 200 deaths and dozens still missing after record levels of rainfall.

Deutscher Wetterdienst, Germany's weather service, reported that many areas of western Germany saw rainfall rates that exceeded a 1-in-100-year return period; or having a 1% chance of occurrence in any given year. DWD noted that some areas may have recorded rains with a 1-in-1,000-year return period; or a 0.1% chance of an annual occurrence.

According to analysis conducted by Aon's Impact Forecasting team, the number of homes impacted across the region runs into the thousands. In addition, infrastructure and business properties were in some cases completely destroyed, in what looks set to become one of the costliest flood events on record.

Aon's report calculated that with storm and flood damage occurring across Switzerland, France, Luxembourg, the Netherlands, Italy, Poland, Hungary, Slovakia and the Czech Republic, the combined cost of the floods and storms across Europe as a whole is expected to run well into the billions.

Variations in insurance take-up mean that while there is likely to be a multi-billion-dollar industry loss in Germany from this event, the overall economic loss will be substantially higher.

"With the event still ongoing across the hardest-hit areas of eastern and central Europe as water levels have yet to fully recede, it remains too early to provide an exact economic loss estimate at this time," Aon noted.

"This will be a continuation of what has been one of the most expensive six-week periods in Europe for the insurance industry in years. A series of severe convective storm outbreaks in late June has already been estimated to result in a combined insured loss of US\$4.5bn. The overall economic loss was even higher at nearly US\$6.5bn."

While acknowledging the devastating consequences of the inundations, catastrophe modellers at RMS said the damage could have been much worse were it not for the measures put in place following past floods.

"As of today, floods have caused devastating and deadly impacts in villages and small cities situated upon minor rivers, as evidenced by the terrible images coming from Belgium, the Netherlands and Germany," analysts noted. "On a more worrying note, the final financial and human impact of these floods are yet unknown as floodwaters are expected to rise further over the coming days, potentially near cities with greater populations.

"Forecasts call for further precipitation to fall and major rivers and lakes are already full; for instance, major lakes in Switzerland have reached or are close to the levels of the devastating 1999 and 2005 floods. In the Netherlands, forecasts expect flows on the River Meuse to exceed that of the historic floods of 1993 and 1995.

"As devastating as the effects already have been, it is important to note that in the wake of past floods, mitigation measures have been implemented across Europe and their performance will have significant influence on how much damage the current floods will cause. The flooding recorded to date would have covered a much more widespread area and caused far more damage than we've already seen, if it were not for these measures already in place."

Indeed, industrial companies on the Rhine have so far not been affected, which should limit the total economic impact, although the damage to the already embattled retail and hospitality sectors could be considerable.



▶ Deborah Ritchie



SUNGARD  
**AVAILABILITY  
SERVICES®**

[sungardas.com](http://sungardas.com)



# Flexible Serviced Workplace Solutions from Sungard Availability Services

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



**100% available  
office space in  
dedicated suites,  
tailored to your  
precise requirements**



**Ability to 'drop in,'  
with badge, to other  
Sungard AS facilities  
across the UK  
and Ireland**



**Fully-hardened,  
facilities following  
best-in-class  
security procedures**



**The option to  
recover to another  
Sungard AS facility**

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

---

► **To learn more about *Serviced Workplace* from Sungard AS please visit [www.sungardas.com](http://www.sungardas.com) or call us on 0808 238 8080.**





# The chips are down

## ➤ SUPPLY CHAIN

### The chips are down

Deborah Ritchie takes a look at the ongoing microchip shortage and considers the impact to supply chain risk management approaches post-pandemic

## DATA PRIVACY

### New resolutions

Following the adoption by the European Commission of revised standard contractual clauses for international transfers, sending data from the EEA to the US has just become a good deal more complicated. By Christian Auty

## CYBER INSURANCE

### Stand and deliver

Lindsey Nelson opines on the issues around cyber risk accumulation, the thorny problem of paying ransoms, and other major developments in the ever-evolving cyber insurance market

## INSURANCE-LINKED SECURITIES

### Political violence capital

Demand for new sources of capital has become salient, leading many to look to the global insurance-linked securities community for support. Tom Johansmeyer writes

16

PI

### The only way is up

Availability of cover, COVID, pricing and claims were recently identified as the biggest problems in the hardest professional indemnity market for years. Despite the challenges, the London Market is bullish about prospects

26

20

## PROFESSIONAL DEVELOPMENT

### Training risk champions

Alexander Larsen explains why risk champions are so crucial in embedding an effective enterprise risk management structure and culture

28

22



24

## BUILDING SAFETY

### The overhaul continues

A major overhaul of UK building safety in the form of the Building Safety Bill will bring about a number of changes that insurers need to be aware of, as Kathryn Turner explains

32

## Editorial & features

✓ A study of terrorist attacks that took passenger rail and bus systems in modern countries between 1970 and 2020 found that 60% of incidents occurred during COVID-19. For the Mineta Transportation Institute's Hour Study, security experts Brian Michalski and Bruce Butterworth analysed more than 100 incidents on both rail and bus systems.

✓ The UK government tested its long-awaited Emergency Alerts system, designed to warn about severe flooding, fires, explosions, terrorist incidents or public health emergencies. Scheduled to launch in summer, the alerts will be broadcast on mobile phone masts to every compatible mobile phone in range, making a loud siren-like sound even overriding silent settings.

✓ Prædicat updated its litigation tracker in 2020 to include three new mass litigations: PFAS (per- and polyfluoroalkyl substances), toxic baby food (heavy metal contamination in baby food) and paraquat (a herbicide alleged to cause Parkinson's disease).

### News, views & regulars

Analysis	8
Book review	9
News in brief	10-13
Industry views:	
Airmic, IRM and GILC	48-49
Executive summary	50
Market Guide: Industry products & services	51

### HEAT STRESS Hot in the city

The number of cities at extreme risk for heat stress is expected to increase by 58% from 482 today to 762 by 2050, as global warming takes hold, according to new research from Verisk Maplecroft

### PODCAST HIGHLIGHTS CYBER INSURANCE IN FINANCIAL INSTITUTIONS With Tokio Marine HCC Hitting the jackpot

How have cyber exposures evolved in the financial sector, and how well are institutions doing when it comes to managing the risks? CIR's latest podcast with sector experts at Tokio Marine HCC covered the key issues

### BUSINESS CONTINUITY AWARDS 2021 The finalists

Congratulations to all of this year's Business Continuity Awards finalists. The countdown to the Gala Dinner and Awards Presentation is on

### NATIONAL INSURANCE AWARDS 2021 The winners!

The winners of the 2021 National Insurance Awards were revealed in July. Hosted by comedian Felicity Ward, the National Insurance Awards showcase outstanding performance in general insurance

**CIR**  
CONTINUITY INSURANCE & RISK

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

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

**Design & production manager**  
Matt Mills  
matt.mills@cirmagazine.com  
Tel: +44 (0)20 7562 2406

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

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

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

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

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

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

CIR Magazine is published by:

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

Tel: +44 (0)20 7562 2400

ISSN 1479-862X  
cirmagazine.com

## Political violence

**Demand for new sources of capital has become salient, leading to insurance-linked securities community for support. Tom Johansen**

The global reinsurance industry seems to be spending more and more time talking about political violence. In addition to the significant implications for insurers have become increasingly noticeable. A clear upward shift in industry-wide insured losses from political violence has led to changes in risk transfer, increased insurer caution, and a salient need for better understanding.

Concern about political violence (especially riot and civil disorder) is relatively new. Reinsurers have watched terror aggregations for years, such events have generally fallen far short of the insured losses caused by natural catastrophe events, such as hurricanes and severe convective storms. In fact, no non-terror political violence event before 2019 reached US\$1 billion in insured losses. Markets stayed small enough to tilt in lower levels of insured

loss, while larger political violence events seemed to occur most often in markets that lacked sufficient insurance penetration.

The 2020 US riots have made the global reinsurance industry view political violence risk with fresh eyes. Known colloquially as the 'George Floyd riot', the event generated more than US\$2 billion in industry-wide insured losses, according to PCS data. Before that, we'd recorded only 12 riot and civil disorder catastrophe events since 1950, with the 1992 riot in Los Angeles the most expensive. At US\$800 million, it was an outlier at the time, given that the average before it was less than US\$50 million.

The US event followed an even larger one in Chile the year before, with insured losses of almost US\$3 billion. At the time, reinsurers were able to perceive it as an outlier because of its size and location. Less than a year later, though, the US event showed characteristics similar to the Chilean event, suggesting an emerging trend. In both riot and

"The 'George Floyd riot' generated more than US\$2 billion in industry-wide insured losses, and made the global reinsurance industry view political violence risk with fresh eyes"

Event	Year	Industry loss
Floyd riot (US)	2021	< US\$150m
"1st" protests (France)	2020	> US\$2bn
riots	2019-2020	€200m
	2019	US\$77m
	2019	~US\$7bn
	2019	US\$50m
	2019	US\$167m

Political violence events (Source: PCS, a Verisk business)

porting, shown as risk coordinators, risk management, and risk business are essentially the same.

The risk champion network is essentially the same.



# EVERYTHING YOU NEED FOR GRC, FULLY INTEGRATED

From ERM to Business Continuity to Compliance Management, unify the entire GRC process. Turn insight into action and monitor progress.



## ORIGAMI RISK

[ORIGAMIRISK.COM](https://origamirisk.com)



# Model behaviour: enhanced climate risk analytics

✓ **The physical impacts of climate change are becoming an increasing concern for both businesses and investors. As Dr Paul Munday explains, enhanced climate risk analytics can provide greater clarity about exposures**

Over recent years, the availability of climate risk analytics has increased exponentially. Aimed at providing entities with a detailed insight into their material exposure to different climate hazards, climate data can help market participants improve transparency and estimate the cost of climate-related risks and opportunities.

Climate service providers have rallied to increase the availability of information with technologies and analytical tools that help entities make sense of this data. However, translating the outputs of climate models into specific potential impacts presents challenges, many of which are compounded by uncertainty and a lack of standardisation.

Financial market participants' information needs often vary – both in terms of the granularity of assessment required and the timing and geographic scales over which climate hazards may play out. As such, the effectiveness of adaptation measures to mitigate exposures are hard to rationalise without a detailed assessment of an entity's past performance and a knowledge of key risk thresholds.

In addition, the rapid uptake of model-driven data has sparked concern regarding the potential unintended misuse of information in financial disclosures – including the potential for misstatements in financial reporting and greenwashing. These risks present a particular threat in the case of long-term capital investments, such as public infrastructure, whose operational lifetime often spans decades.

## Optimising climate data

In the absence of a universal solution to bring analytical approaches into alignment, there are processes that can be prioritised to optimise current practices. Greater standardisation, through the development of consistent terminologies as well as the definition of appropriate use cases and parameters, could enhance comparable assessments of climate-related risks and opportunities and their potential impacts, in turn supporting better analysis of an entity's vulnerability to the physical impacts of climate change.

In addition, applying multiple scenarios to assess climate-related risks and opportunities can also help decision-makers consider a broader range of possible outcomes. Indeed, multiple scenarios have long been used as a tool to build organisational resilience, and in the case of climate risk analytics, they can help enrich dialogue about longer-term risks and the interventions that may be required to mitigate them.

Finally, enhanced climate risk analytics – which involve supplementing outputs of climate models with entity-specific data – can facilitate market participants' understanding of both the financial and physical repercussions of climate change for their businesses.

## Climate modelling: the next step

As the costs of extreme weather continue to mount, the next generation of climate risk models will need to be more innovative. Climate hazards are often not isolated events, and therefore the potential for new, more complex interdependencies that existing, siloed models are unable to resolve presents a real threat.

Integrated assessment models offer a potential solution by grouping together multiple models to resolve the impact chains connecting environmental, socioeconomic and climatic systems. They are also able to help rationalise the effects of greenhouse gas mitigation efforts and the costs associated with various climate policy targets. Non-equilibrium models, which assume a more complex relationship between climate variables, present another viable alternative, and can also leverage multiple scenarios as part of sensitivity testing.

Of course, these solutions do not come without their own set of challenges. IAMs are typically calibrated to the change in global mean temperature, limiting the insights they can bring on changes in local extreme events, such as storms and flash flooding. Additionally, such models are relatively complex for non-experts and expensive to run – meaning the challenges that undermine existing models are likely to affect the future generation.

Despite limitations, enhanced climate risk analytics can play an important role in building entities' resilience to the physical impacts of climate change. Indeed, analytics can improve transparency and foresight about potentially material exposures, while avoiding the unintended misuse of climate model outputs by financial market participants.

This, in turn, will provide corporates with a much more thorough understanding of how climate-related risks may threaten their businesses, enabling them to better prepare for a range of potential outcomes.



Dr Paul Munday is a director at S&P Global Ratings



## Inspiration for resilience professionals

**CATASTROPHE  
and Systemic Change**Learning from the Grenfell Tower  
Fire and Other DisastersGill  
Kernick**➤ Catastrophe and Systemic Change: Learning from the Grenfell Tower Fire and other Disasters**By Gill Kernick, London Publishing Partnership, 2021  
[londonpublishingpartnership.co.uk](http://londonpublishingpartnership.co.uk)

The Grenfell Tower tragedy was the worst residential fire in London since World War II, killing 72 people in one of the world's wealthiest neighbourhoods.

Surely, then, lessons will be learned from it, and lasting change implemented.

Unfortunately, as history tells us, the evidence is weighed against this outcome – indeed, four years after Grenfell, the UK's cladding issue remains unresolved, putting the lives of thousands at risk and on hold.

This book seeks to understand why there is a persistent failure to learn from catastrophic events. Published near the anniversary of the tragedy, *Catastrophe and Systemic Change: Learning from the Grenfell Tower Fire and other Disasters* lays out the many failings that led to the deadly inferno.

This powerful book examines the challenges and conditions that inhibit learning, with the goal of finding opportunities to disrupt the status quo.

Author Gill Kernick is an internationally experienced strategic consultant specialising in safety, culture and leadership. She also lived on the twenty-first floor of Grenfell Tower between 2011 and 2014.

In this book, Kernick offers an accessible model for systemic change in the form of a framework to evoke reflection, enquiry and debate.

The book is organised in two parts: the first focusing on

the Grenfell Tower fire itself, the second dedicated to analysis and reflection – seeking to understand why our failure to learn makes sense by exploring the reasons why, and asking what it would take to enable real systemic change.

Subsequent chapters explore the issues of catastrophe and systemic change through a number of different 'lenses', among them behavioural and relational elements. The author shares stories of other catastrophic events, considers some widely-held myths, reflects on insights from Grenfell, proposes the conditions that prevent change, and looks at the key opportunities to positively disrupt the status quo.

In praise of *Catastrophe and Systemic Change*, Her Honour Frances Kirkham CBE (coroner in the Lakanal House inquests) points out that learning from catastrophic events to drive necessary change should happen in every area where public safety is a fundamental requirement, as, for example, in the provision of housing.

"It is scandalous that there is widespread and fundamental failure to apply any lessons learned," she says. "Read this book to understand the interplay between those at the top and those at the bottom of the power ladder, and understand how we all can, and should, influence decision and policy makers to facilitate and achieve the changes which are so needed."

This book will be essential reading for those interested in change management, leadership, policymaking, law, housing, construction and public safety and politics.



## News briefing

### > A round-up of the latest industry news

✔ The total value of Europe's 500 most valuable brands dropped by 10% during the COVID-19 pandemic – from €1.96trn in 2020 to €1.76trn in 2021, according to a global study conducted by Brand Finance. The top 500 brands in the US have a total brand value of €3.40trn. China's are valued at €1.65trn.

✔ More than half of firms faced at least one third-party risk incident whilst responding to the pandemic, some 13% of which were considered 'high impact', compromising financial performance and profitability, and even regulatory compliance, Deloitte said.

✔ Business group the CBI hailed the return of businesses confidence to the UK, forecasting a breakthrough year for the economy, despite the government's decision to delay the final step of its 'roadmap' out of lockdown. The easing of most pandemic-related restrictions in line with Steps 1 to 3, rapid vaccine roll-outs and the unleashing of pent-up consumer demand were behind the numbers.

✔ The Health and Safety Executive continued its surprise visits to UK businesses to ensure workplaces are COVID-secure, warning employers they face action and even prosecution if they are found to fall short of the expected level of risk management.

✔ Organisations have a "once in a generation" opportunity to change working practices for the better, according to the Chartered Management Institute, as it published research suggesting that only half of UK firms had consulted with staff about the big return to the workplace, leaving the rest at risk of reverting to the "old normal".

✔ Three years after GDPR came into force, UK security professionals are more concerned about class action lawsuits following a serious data breach than they are about regulatory fines. Half of consumers said they would be prepared to join a class action lawsuit against a firm that had leaked their data, suggesting that security professionals' fears are not misplaced.



✔ Business groups in the UK welcomed the launch of flexible season tickets on the UK's rail networks, hailing the new approach a win for hybrid workers as well as for the climate. The CMI said the move was precisely what the changing workforce needed. Other groups expressed their disappointment with the scheme, which, for many commuters, appeared to offer no saving whatsoever.

✔ Pool Re cautioned that the lifting of lockdown restrictions and increased passenger numbers heralds the return of crowds and, with it, the potential for terrorist attacks. Counter-terrorism police have issued a number of warnings relating to the increased threat of self-radicalisation during lockdown.

✔ A study of terrorist attacks that took place on passenger rail and bus systems in modern developed countries between 1970 and 2020 found that more than 60% of incidents occurred during off-peak hours. For the Mineta Transportation Institute's latest *Peak Hour Study*, security experts Brian Michael Jenkins and Bruce Butterworth analysed more than 500 attacks on both rail and bus systems.

✔ The UK government tested its long-awaited Emergency Alerts system, designed to warn the public about severe flooding, fires, explosions, terrorist incidents or public health emergencies. Scheduled for launch in summer, the alerts will be broadcast from mobile phone masts to every compatible mobile phone or tablet in range, making a loud siren-like sound, even overriding silent settings.



For the full story behind all these headlines, visit [cirmagazine.com](http://cirmagazine.com)

✔ The US government issued emergency legislation after a ransomware attack forced the shutdown of the crucial US Colonial pipeline, which supplies almost half of total East Coast consumption of diesel, gasoline and jet fuel. The emergency status relaxes rules on fuel being transported by road. The cyber attack served as a reminder of the potential cyber risk accumulation around vital infrastructure or technology systems.

✔ Personal data may continue to flow freely between Europe and the UK following agreement by the European Union to adopt 'data adequacy' decisions, which mean that organisations in the UK can continue to receive personal data from the EU and EEA without having to put in place additional arrangements with European counterparts.

✔ Computer networks at the world's largest meat processing company, JBS, were hacked, temporarily shutting down some operations in Australia, Canada and the US. The company paid the equivalent of £7.8m in ransom to put an end to the attack. The payment was reportedly made using Bitcoin. The firm said it was necessary to pay to protect customers, with chief executive, Andre Nogueira adding that the decision was very difficult both for the company and for him personally.

✔ A poll among security professionals indicated that a large proportion of firms that chose to pay ransom demands went on to suffer a second attack – often at the hands of the same threat actor. In the UK, 84% of organisations that paid a ransom demand were hit again, with 61% reporting significant loss of revenue.

✔ Companies in the technology, media and telecoms sectors, financial institutions and healthcare and life sciences companies feel more resilient now than they did 12 months ago, whereas those in the hospitality and entertainment sectors feel quite the opposite. This is according to a study conducted by insurer Beazley, which identified cyber risk as highest on leaders' lists of concerns. However, they also feel relatively well prepared to handle it, with 44% feeling 'very prepared'.

✔ Axa launched a settlement offer to 15,000 restaurant owners in France with non-damage business interruption insurance. The insurer said it expects that these settlements will be around €0.3bn before tax and reinsurance (likely to be a lower bottom line impact post tax and reinsurance).

✔ Praedictat updated its litigation tracker in CoMeta to include three new mass litigations: PFAS (per- and polyfluoroalkyl substances), toxic baby food (heavy metals in baby food) and paraquat (a herbicide alleged to cause Parkinson's disease).

✔ A leakage of nitric acid, which was correctly declared but apparently incorrectly packaged or packed, was thought to have been the catalyst for a fire on Singaporean Super Eco 2700-class container ship, X-Press Pearl. Shipping experts at TT Club said the incident underlined the continuing problem of ship fires caused by the mishandling of dangerous cargoes. One estimate puts the number of mis- or undeclared dangerous cargoes in excess of 150,000 containers a year.



## News briefing

### > A round-up of the latest general insurance news

✔ The most successful insurers have a number of factors in common, including 'thoughtful growth', a focus on markets in single countries and digital maturity. This was among the findings of a study conducted by Acord and Alchemy Crew on the primary drivers of success among 40 of the largest insurers headquartered in Europe.

✔ Aon's proposed US\$35bn purchase of Willis Towers Watson is being challenged by US antitrust regulators, who say the proposed merger would eliminate competition and lead to higher prices and reduced innovation for customers in the US.

✔ Data from the Financial Conduct Authority shows that insurers have settled 43% of accepted COVID-19 business interruption claims, following the test case and appeal contested by the regulator. So far, insurers have paid £268m in interim payments and £467m in final settlements.

✔ UK motor insurers achieved a 90.3% net combined ratio in 2020, following the unprofitable 100.8% recorded the previous year, according to consultancy EY's latest *UK Motor Insurance Results*. It forecasts a return to the red in 2021 and a net combined ratio of 103% for the market. It expects this to deteriorate further in 2022 to 112%.

✔ The Financial Conduct Authority opened a consultation (CP21/13) on its plans to introduce a higher level of consumer protection in retail financial markets. It said the new duty will ensure that consumers always get products and services that are fit for purpose, that represent fair value and are clearly communicated and understandable.

✔ HRH The Prince of Wales launched a Sustainable Markets Initiative Insurance Task Force, which aims to provide "climate positive financing and risk management solutions to support and encourage individuals and businesses around the world to accelerate their transition to a sustainable future".

✔ The Association of British Insurers and Flood Re highlighted the value of maintaining flood defences in the UK ahead of the government's consultation on its comprehensive spending review. A joint report found river flood defences provide protection valued at £568m a year and that every £1 spent on flood defence maintenance, saves £7 in spending on new defences.

✔ Rating agency Moody's said European insurers have been 'relatively unscathed' by COVID-19, despite some significant and unexpected losses, and must now prepare for post-pandemic challenges. It highlighted the accelerated switch to digital and the gap between policy cover and customer expectation as particular issues, and predicted an uptick in sector M&A activity as carriers seek refuge in scale.

✔ Carpenters Group joined the Managing General Agents' Association as a supplier member. The legal firm provides claims services to insurers, brokers and MGAs. The arrangement will give members access to the firm's service such as FNOL claims handling and defendant litigation services.

✔ The Lloyd's Market Association unveiled findings from its six-month project, Dare, carried out in partnership with consultancy 6point6, to offer a reimagined model for delegated authority business. The work included 45 group workshops and 12 SME interviews with over 330 attendees, supplemented by online surveys with over 200 responses.





For the full story behind all these headlines, visit [insurancetoday.co.uk](https://insurancetoday.co.uk)



✓ Swiss Re sold a stake of around 6.6% in Phoenix Group Holdings plc for £437m. The shareholding was acquired in the sale of ReAssure in 2020. Swiss Re said the sale was part of a regular review and rebalancing of its investment portfolio and is consistent with its overall investment strategy across equity and alternative investments.

✓ Covéa rolled out Iotattech's new Policy Platform across its motor business. The new platform offers full policy lifecycle management, promising highly configurable workflows and integration with affinity partner, third party and legacy systems.

✓ Specialist insurer, Peach Pi announced a partnership with Tapoly to create insurance for freelancers and micro SMEs operating in the health and well-being sector. The new product is available online and includes cover for professional indemnity, public liability and treatment risk.

✓ Covéa Insurance agreed a deal with water leak detector, Leak Bot to roll out its devices to the insurer's high net worth customers across the UK through its broker and affinity networks. The new deal builds on an existing relationship that began in 2017.

✓ London-based MGA Rising Edge officially launched, after announcing its creation earlier in the year. It specialises in D&O. Vantage Risk, the Bermuda-based Class 4 reinsurer, will provide reinsurance capacity. Accredited Insurance will provide the required insurance licenses to underwrite business.

✓ The majority (86%) of SMEs in the UK are operating without cyber cover, according to Aviva. Research by the insurer found significant regional variation with just 3% of Scottish SMEs having cyber insurance compared with almost a third (32%) in Northern Ireland.

✓ Insurer Chubb launched a pay-as-you-roam travel insurance proposition, which uses mobile phone roaming data to identify when customers are away from their home country to activate coverage automatically at a daily premium.

✓ CPP Group UK partnered with NPA Insurance to run the claims and 24/7 emergency helpline service for its new key insurance offering.

✓ RSA announced plans to join digital broker Simply Business's panel of providers. It will offer insurance products to Simply Business's customers through the More Than and RSA brands. The insurer will also offer its RSA Shop insurance to help meet growing online demand from shop owners.

✓ The FCA implemented changes to prevent a renewal quote for home and motor insurance being more expensive than it would be for a new customer. The pricing, auto-renewal and data reporting remedies come into effect on 1st January 2022.

✓ Howden announced the launch of Parhelion, which it said will be the world's first fully sustainable insurer. Parhelion is targeting a capital raise of around £350m and will implement an underwriting approach based on data, technology and proprietary ESG criteria. It aims to start underwriting from 1st January 2022.

✓ London-based underwriting agency, Attento opened its doors for business. The agency deals in commercial motor and associated products in the US and Canada and offers the surplus lines markets an alternative solution for their insurance requirements.

✓ IDEX Consulting completed its merger with Aspects Insurance Recruitment, the consultancy set up by Allison Marshall in 2007.

# The ESG illusion

✓ In complex product categories, ESG risks run high. Deborah Ritchie speaks to TCO Development's Clare Hobby about the role of independent verification in stamping out greenwash

**Whilst it's not a new concept, scrutiny over perceived greenwashing appears to be on the rise. How does the issue manifest in the IT sector and across business as a whole?**

The world is becoming much more conscious of ESG commitments, and the private sector has now realised they have a part to play. It is no longer a 'nice to have'. It has become a core part of doing business.

So there is an enormous amount of greenwashing going on as there are a lot of loopholes and shortcuts being taken. At the same time though, there's a lot of good, authentic work being done. So currently there are lots of different levels of maturity.

At TCO Certified, we are specifically focused on IT. Governments have long been in a leadership position in this space as they have sustainability mandates, so they're typically early adopters of sustainable hardware procurement.

Most of the work we do is with large corporations and large governmental buyers – organisations that are under a lot of pressure in the ESG space. They take on an awful lot of risk in the products that they buy at scale.

Take battery life claims, for instance. We have seen examples of notebook computers that the manufacturer has claimed can last up to 800 or so full battery cycles, when in fact they only last up to approximately 300. If you are buying 2,000 of these machines for your organisation, you can start to see the impact of that lifecycle. These kinds of greenwashing issues come with

real cost risk and credibility risk.

Clarity and transparency over chemical content is another issue. Today, only around one per cent of all chemicals have been tested for any kind of human health and environmental hazard. This is one of a number of areas that really need to be under greater scrutiny than they currently are. Buyers do not currently have a way to do this. We want buyers to know that it is important to ask these questions.

**“Sustainability work takes time and is an exercise in long-term continuous improvement if greenwash is to be avoided”**

We began a conversation some time ago with the chemicals manufacturing industry (a notoriously secretive industry) as part of our ambition to create a public list of safer alternatives, which goes beyond just banning the most hazardous chemical substances. Whilst it was a real challenge to begin with to get this level of transparency, we persevered and several chemical manufacturers have now reached a point where they have begun to see the benefits to business. This demonstrates how this really tough problem can be tackled to the benefit of all – industry, users and purchasers alike.

**Is greenwashing more about marketing spin or cost-saving?**

It is a bit of both. Product manufacturers worldwide know that most of their customers want

them to 'figure out' sustainability.

Customers everywhere are asking for all this information, and the work simply can-not be done overnight. Sustainability work takes time and is an exercise in long-term continuous improvement if greenwash is to be avoided. It's not a quick fix that marketing spin can address. At the same time, we need to reconcile the push for more sustainability with the continuing desire for low cost, quick to market products.

Some organisations have been doing lots of great work and genuinely can make these claims, but for others to get access to contracts and tenders, they may be relying on a bit more greenwashing in order to get that sale. It's important that purchasers have access to tools that help them tell the difference and make an informed product choice, where sustainability claims are independently verified.

We often tell companies they should not expect a clean supply chain overnight. It is more about continuous improvement. All audits will find something that you do not want to see – but that is the work. You need time, patience and access to tools that help you do it right.

**In how much detail should sustainable procurement efforts be reported on?**

This is a really evolving space. There is a lot of work happening amongst procurement organisations around the degree to which efforts can be measured. It can start with something very simple like working out how much of a company's budget can





Clare Hobby, global purchaser engagement lead at TCO Development

be categorised as being 'sustainable spend'. A lot of organisations are starting there. Others are looking at how much energy they have saved or how much waste they are diverting. Efforts like these are fairly straightforward and accessible.

At the other end of the scale are Scope 3 emissions, where a company not only looks at its own emissions, but those of its suppliers, too. In the case of IT, for instance, 80 per cent of lifetime emissions happen when a laptop or phone, or other hardware is in the supply chain – not when it's on the end-user's desk.

#### Do consumers care?

Surveys suggest they do. When it comes to electronics, however, a lot of those concerns go out of the window at the point of purchase. Like it or not, consumers see a glossy new mobile phone or the latest TV, and excitement takes over. The consumer is a really, really ambitious target for us to reach. We have chosen to work firstly with the volume buyers and of course want to also inspire consumers to follow suit.

Consumers and volume buyers alike need some kind of objective measurement. If we are leaving it up to each brand to declare what their emissions are, then it makes

it difficult for buyers to compare machine to machine. If you leave it up to what the brand is telling you, that carries a risk.

Too often, buyers are forced to rely on what manufacturers tell them. Some of it is true and some of it is not! For purchasers to signal to companies that this is where they want to see change is very powerful.

We saw a similar trend in the drive to recycle, but we need to go even further. The focus needs to be firmly on repairing and reusing.

Recycling is a step in the right direction, but it is not the goal and is highly energy-intensive. Continuing to buy things because we can recycle them it is a bit of a false narrative.

Just this month, the UK

**“If we leave it up to each brand to declare their emissions, it makes it difficult for buyers to compare machine to machine”**

government introduced new 'right to repair' rules that legally require manufacturers to make spare parts available to buyers of electrical appliances. Europe and the US look set to follow suit with similar orders in the pipeline on both sides of the Atlantic.

#### Mixed wash

The term 'greenwashing' was reportedly coined in 1986 by environmental activist, Jay Westerveld, in response to the perceived motive behind a hotel's request to guests to reuse their towels. Some 35 years later, the term is used widely to cover misleading claims made about environmental or sustainability efforts.

Along similar lines, 'bluewashing' relates to unvalidated social claims (sometimes referred to as 'redwashing'); and cleanwashing refers to branding that makes products, such as food and cosmetics, seem healthier than they really are to tap into clean living and wellness trends.

#### What's next?

What we know for sure is that the reason manufacturers want to apply for TCO Certified for their products is to show their sustainability credentials and meet their customer requests. This work doesn't just happen by itself – the voice of the purchaser is an important driver.

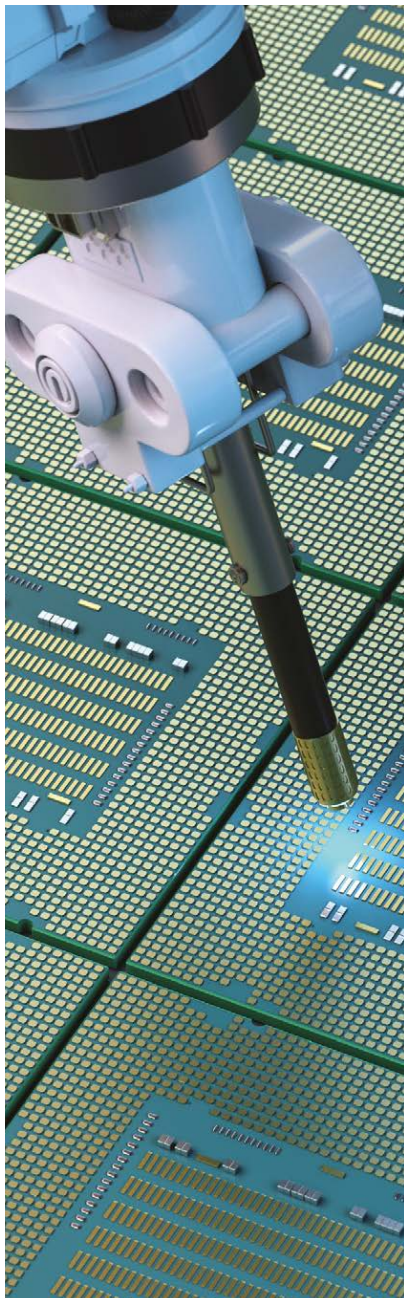
IT products come from a complex, global supply chain, which is largely not accessible or visible to the large majority of purchasers. The issue is that it's in this supply chain, where much of the sustainability impact lies. So it's important that purchasers have access to tools that are backed up by the expertise and verification resources on the ground to assess that responsible practices are being implemented throughout.

Customers need to know that if they buy products from a particular manufacturer, that it has not been made in a facility where child labour or forced labour is in place, or in a factory where staff are made to work excessive overtime, have health and safety hazards, or even locked fire exits. And it might not be obvious, but forced labour still exists in the supply chain.

**Interview by Deborah Ritchie**

# The chips are down

**Deborah Ritchie takes a look at the ongoing microchip shortage and considers some of the broader developments in supply chain risk management approaches post-pandemic**

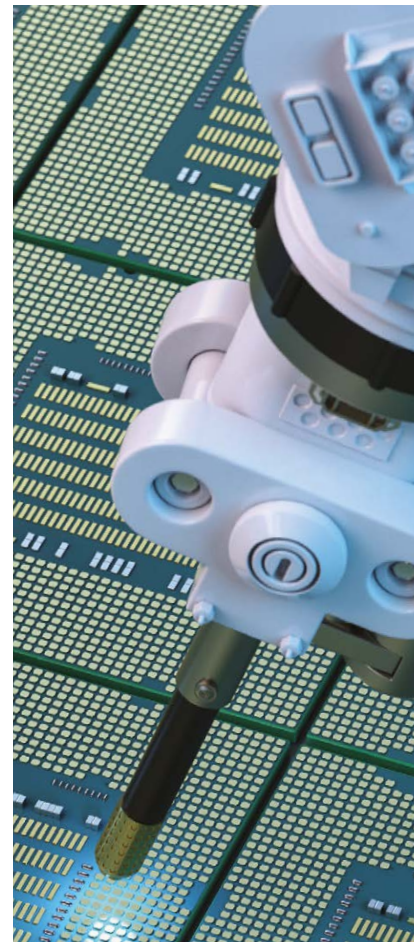


Devoted Samsung fans will have been disappointed by the company's recent admission that the ongoing global shortage of semiconductors had been a contributory factor in the decision to delay the release of its much-loved Galaxy Note smartphone, which had been slated for release later this year.

The electronics giant has been struggling to manage what it described as a "serious imbalance" in global supply, with CEO, Koh Dong-Jin, warning shareholders that the supply problem could continue into 2022.

Global demand for semiconductors has been on a steady rise, boosted in part by strong sales of PCs, smartphones and games consoles. Increased home-working has also seen demand for technology at home rise substantially, and quickly. The chip shortage has had a widely reported impact on the automotive sector, with Toyota, Honda and Volkswagen among the manufacturers affected.

Throughout the global pandemic and geopolitical tensions of the past year, it has been the companies with the leanest, and seemingly most efficient, global supply chains that have suffered the greatest disruptions. Meeting soaring customer expectations for faster delivery, customisation, lower cost and sustainability are considerable challenges for these inflexible networks.



To address this, some companies are working on building more resilient, flexible supply chains, underpinned by real-time insights. As a recent Bain and Company brief notes: "The traditional practice of upgrading and replacing supply chain backbone technology every 12 to 15 years is far too slow to meet urgent new challenges. Starting a multi-year transformation today risks producing



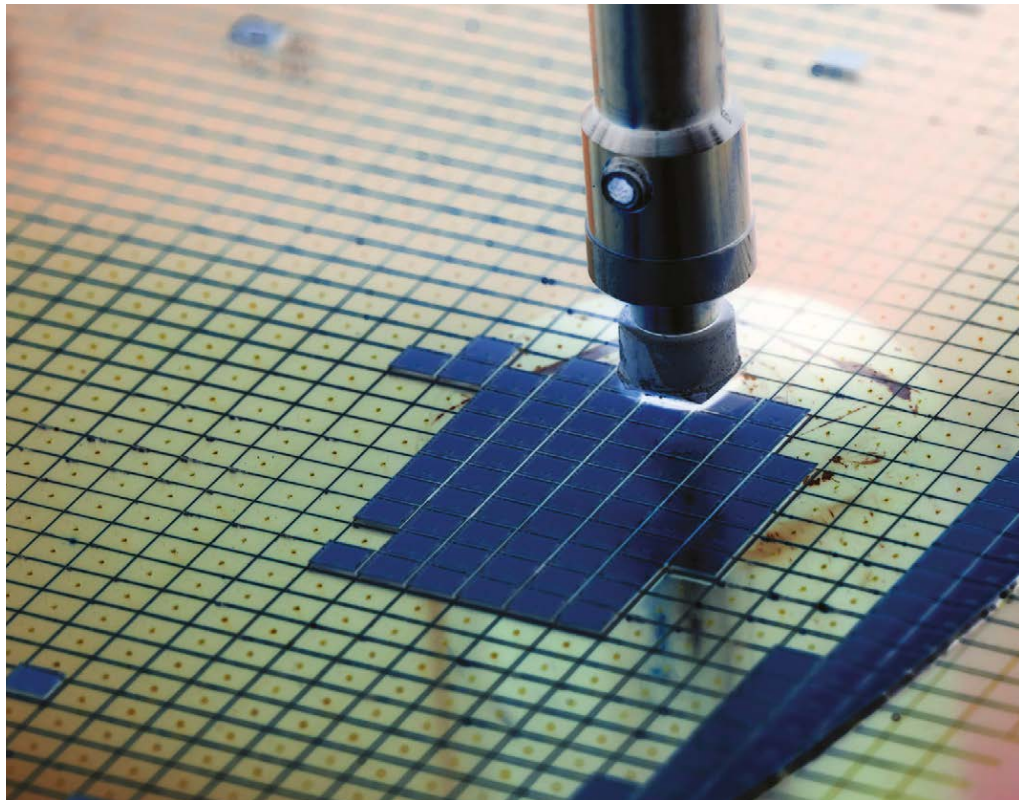
a technology backbone that's obsolete as soon as it's launched. It also will be unable to integrate innovative digital solutions quickly in response to market changes."

Partners at the company, Olaf Schatteman and Juliane Stephan, say that leaders can overcome this hurdle by taking a more adaptive approach – by deploying rapidly evolving technologies, including cloud-based software-as-a-service applications, that continually enhance the supply chain backbone. Artificial intelligence, machine learning and advanced analytics also help to improve forecasting and network optimisation. Bain says companies engaged in this approach understand that an adaptive technology architecture is the foundation for a more resilient supply chain – and a powerful competitive advantage.

"In our experience, leaders get two things right: they opt for a core-light architecture and embrace agile ways of working. The technological and organisational moves are interdependent. An agile, 'test and learn' approach to innovation requires a technology architecture that can adapt easily to change, such as a cloud-based system that offers software as a service. Similarly, an adaptive technology approach can achieve its full potential only when companies manage supply chain processes from end-to-end. That means eliminating silos that separate functions, business units, and countries."

### **Solution becomes the problem?**

More than half of firms faced one or more third-party risk incidents whilst responding to the pandemic, some 13 per cent of which were considered 'high impact', severely compromising financial performance and profitability, customer service and, in



some instances, putting organisations in breach of regulations.

This was among the findings of a study carried out by Deloitte, which also found that, one year on from the start of the pandemic, half of firms remain in 'respond' mode in dealing with the impact of COVID-19, leaving many of them vulnerable to further third-party failure. Some 27 per cent of organisations that had not adequately invested in third-party risk management prior to the pandemic faced a high-impact incident during the crisis, compared with just two per cent for those that had.

Commenting on these findings, Kristian Park, extended enterprise risk management partner at Deloitte, says: "As businesses have shifted to more digital ways of working, new technologies and the continued need to both reduce costs and access specialist skills have bred a new set

of risks when it comes to third-party oversight. Whilst many organisations have long-established third-party risk management programmes in place, the COVID-19 pandemic has highlighted unforeseen gaps, making many vulnerable to failures caused by third parties – for which the organisations are, ultimately, responsible. As a high proportion of respondents remain in 'respond' mode to the pandemic, it suggests many underestimated their preparedness to deal with such an event.

"One area in particular that most organisations identified as a priority was digital risk. With many workforces moving to remote locations, some for the first time, this has opened up greater opportunities to fall victim to cyber crime. Many organisations won't have considered the security policies and guidelines

## Supply chain risk post-pandemic

**The global pandemic raised customer and third-party risks, and consequently altered risk posture across many regions and industries. CIR asked Charles Minutella, head of Due Diligence at Refinitiv, for his views on the changes.**

### How are technologies helping to manage supply chain risk in the post-pandemic world?

Data and technology will play a major role in managing supply chain risk going forward. The pandemic exposed how fragile supply and distribution networks had become, considering all the disruption we experienced in the early days of the pandemic. Companies had to deal with a range of issues, including demand shifts, product and labour shortages and mobility restrictions.

This led many companies to shift long-standing strategies: first to stabilise their networks through the addition of new suppliers to meet short-term demand. Next, they pivoted towards building more resilience into their programmes by introducing multiple third-party vendor and distributor strategies, so that their businesses could adapt to events that caused disruption, whether a natural disaster, a geopolitical situation, or unforeseen incidents, such as the incident in the Suez Canal a few months ago.

To adequately manage this in the future, companies will need supplier risk technology to centralise the on-boarding and relationship lifecycle management of their suppliers. They will need to identify a wider set of risks at the outset and use data to manage the ongoing change in risk profile the supplier presents. We also see customers investing in key data sets to identify traditional and emerging risks, such as identity, integrity, ESG, financial, cyber and operational risk.

They then need to be able to react to changing factors in real time, which can't be done without consistency in processes and technology to enable the identification of issues. Without technology and data, companies will struggle to ensure resilience and sustainability in their supply chains.

### What are the key differences in attitudes towards SCM before and after the pandemic?

What's come out of the pandemic is quite fascinating, in that during one of the most difficult and uncertain times in history, companies made very public commitments to operating in a more sustainable way. COVID was an element of it, but it's mainly down to pressures coming from internal stakeholders, investors, customers and employees to act in a more ethical, conscious and socially aware way.

Clearly, the agenda has become broader, and the expectation

that companies act in a more responsible way is a board-level issue. SCM is no longer a cost and operational function; it is also about ensuring that the way suppliers operate is in line with the CSR goals of an organisation. Companies that operate in a sustainable and ethical way are performing better, and they are seeing greater investment and customer and employee preference, so there is an overwhelming number of arguments for operating in a sustainable way. This year, for example, Apple made a commitment to aligning a portion of executive compensation to achieving CSR goals – a step in the right direction to align reward to delivering on these ambitious goals.

### Which changes will endure as the world transitions away from operating amid the pandemic?

Companies will continue to prioritise their transformation towards a sustainable future and supply chain will be a big area of focus, as stakeholders increasingly realise that an overwhelming exposure to sustainable and ethical operations risk sits in third-party networks. The UN published a report a few years ago that showed that in technology, healthcare, consumer products and automotive, up to 95 per cent of environmental and ethical risk exposure was in third party networks.

Unfortunately, most companies are not identifying and mitigating these risks, as on average (according to a survey we conducted last year), only 43 per cent of third parties undergo any sort of due diligence.

### How will the ongoing microchip shortage issue play out in the coming months?

Key players like Intel, Samsung and TSMC have announced investment and diversification programmes, but the fact remains that 70 per cent of semiconductor manufacturing comes from Samsung and TSMC, with a heavy concentration in operational footprint in specific locations. By all accounts, these companies continue to scale up production but with pent-up demand and uncertainty around the impact of COVID variants, it will be difficult to predict if supply will improve in the short-term.

### How can such issues be avoided moving forward?

There is a much bigger emphasis on supplier diversification to prevent single source or geographic risk. To significantly overhaul a supply chain will require a retooling of an ecosystem that has been focused on optimisation for decades. Leaders will have to decide how to introduce these themes into their operations while dealing with potential pressures such as inflation, business and stock performance.

that a remote workforce – and, by extension, third parties – required until now.”

A separate study, this time from Refinitiv, suggested that only 44 per cent of organisations conducted third-

party due diligence checks during the pandemic. Respondent organisations reported being under mounting pressure to increase revenue (73 per cent) and profits (65 per cent) due to the pandemic. As their organisations

were burdened to keep operations and disrupted supply chains running, a staggering 65 per cent took shortcuts with KYC and due diligence checks – significantly increasing their risk exposure.



When it comes to due diligence checks, by region, Europe was the lowest performing (40 per cent) while Sub-Saharan Africa (56 per cent) the highest.

A focus on rapidly forging new third-party relationships also created an environment with reduced sanctions screening, with only 40 per cent of organisations making screening a priority and 56 per cent of respondents admitting they did not fully manage risks related to sanctions screening.

Regulators also eased the pressure. Compared with Refinitiv's 2019 report, pressure from governments (75 per cent), regulators (67 per cent) and corporate boards (64 per cent) was considerably lower during the pandemic.

"COVID-19 plunged many organisations that already had fragile third-party networks into an uncertain, turbulent and very competitive market and forced them to rapidly expand their vendor network as they struggled to protect critical supply chains from disruption. Looking back at the lessons learned over the past 16 months, it is clear that businesses must close the compliance gap and focus on building a resilient supply chain with due diligence and financial crime prevention at its core," says Phil Cotter, global head of Customer and Third-Party Risk, Refinitiv.

"As organisations slowly recover from the COVID-19 impact, we expect an increase in technology investment as they seek new ways to address customer and third-party risk challenges."

### Recovery underway

While the pandemic-induced microchip shortage continues to impact production, global car sales showed a recovery in the first half of this year, with analysts forecasting

### Diversity in the supply chain

In other supply chain related developments, a recent Bain Insights brief examined how supplier diversity goals may be more effectively implemented into procurement strategies.

Partners Radhika Batra, Jason Housh and David Schannon note that, in addition to being good for society, a diverse supplier base is said by a growing number of executives to have improved business performance:

"UPS, Target, Pacific Gas and Electric, and other leaders have been building more diverse supplier pools for decades, a move that benefits their bottom lines and reduces supplier turnover. Companies that make up the top quartile in percentage of spending on diverse suppliers generate more

procurement savings than the average company engaging diverse suppliers...

"UPS spends US\$2.6 billion annually on contracts with 6,000 small and diverse suppliers and is committed to growing that pool. To strengthen organisational alignment, the leadership team established a diversity and inclusion council that oversees execution, ensuring executives meet the board's objectives to increase annual spending on diverse suppliers.

"The council helps identify conflicts in messaging and processes, and it was instrumental in convincing key stakeholders, including other business units and functions, to view diverse suppliers as potential sources of innovation."

### "Logistical issues are not likely to disappear in the short-term as supply is still having trouble keeping up with demand"

growth of up to nine per cent in light vehicle sales in 2021.

"We believe that the continued headwinds from the chip supply shortages may slow and should not deter the recovery, while electrified vehicle sales continue to expand," analysts at ING stated in a recent briefing note. "In our *Automotive Sector Outlook*, published in January, we outlined expectations for global passenger car sales growth of seven per cent to nine per cent in 2021. At the mid-point of the year, we are inclined to maintain this range, in spite of the continued supply chain headwinds experienced by car manufacturers. While some statistics for the first six months are still being finalised, we believe that things are progressing broadly as we expected with the recovery in sales, underpinned by solid consumer demand in major geographies."

Despite this upbeat projection, ING says sourcing issues with the supply of semiconductors are proving to be a "more lasting phenomenon" than industry commentators perhaps expected at the start of the year.

"As we have crossed the half-year mark, we feel that the visibility on the matter is still rather limited with new commentaries appearing almost daily and frequent updates provided on the sales and production impact. What can be noted is that the semiconductor shortages have already left a mark on the first half 2021 car manufacturer production and sales volumes and, also, the logistical issues are not likely to disappear completely in the short-term as supply is still having trouble keeping up with demand.

"...we may be on the cusp of semiconductor supply turning and things improving gradually. While the worst may be behind us, it is unlikely that things will return completely to normal during the remainder of this year."

**Deborah Ritchie is editor of CIR Magazine**

The GDPR requires all transfers to be supported by an 'adequacy measure'. In practice, there have been two popular approaches for transfers to the US: (i) the Privacy Shield mechanism and (ii) the Standard Contractual Clauses. But for more than a year, transfers of personal data from the European Economic Area to foreign countries, and the US in particular, have been under heavy pressure. Indeed, some commentators believe such transfers may one day be impossible due to further regulation and decisional law in the EEA.

This is so because, nearly one year ago, the Court of Justice of the European Union invalidated the EU-US Privacy Shield mechanism for data transfers from the EU to the United States. That decision, known as Schrems II, reaffirmed the use of the so-called Standard Contractual Clauses to effect such transfers. After Schrems II, SCCs became the default mechanism by which EU legal entities transferred personal data to the US. Other mechanisms exist but are rarely used for pragmatic reasons.

In practice, the legal entity sharing data outside the EU would execute the SCCs as the 'exporter' and the recipient would execute the SCCs as the 'importer'. The terms of the SCCs were set in stone. This act was required of both parties when personal data left the EEA to be stored or processed in the US (and most other countries).

But while the ruling in Schrems II reaffirmed the use of SCCs, the opinion criticised their use relative to data transfers to the US, and called upon European regulators to take a renewed look at such transfers. There was accordingly general scepticism in the data privacy community regarding whether the protections in the SCCs, by themselves, would be sufficient



# New resolutions

**Following the adoption by the European Commission of revised standard contractual clauses for international transfers, sending data from the EEA to the US has just become a good deal more complicated. Christian Auty explains**

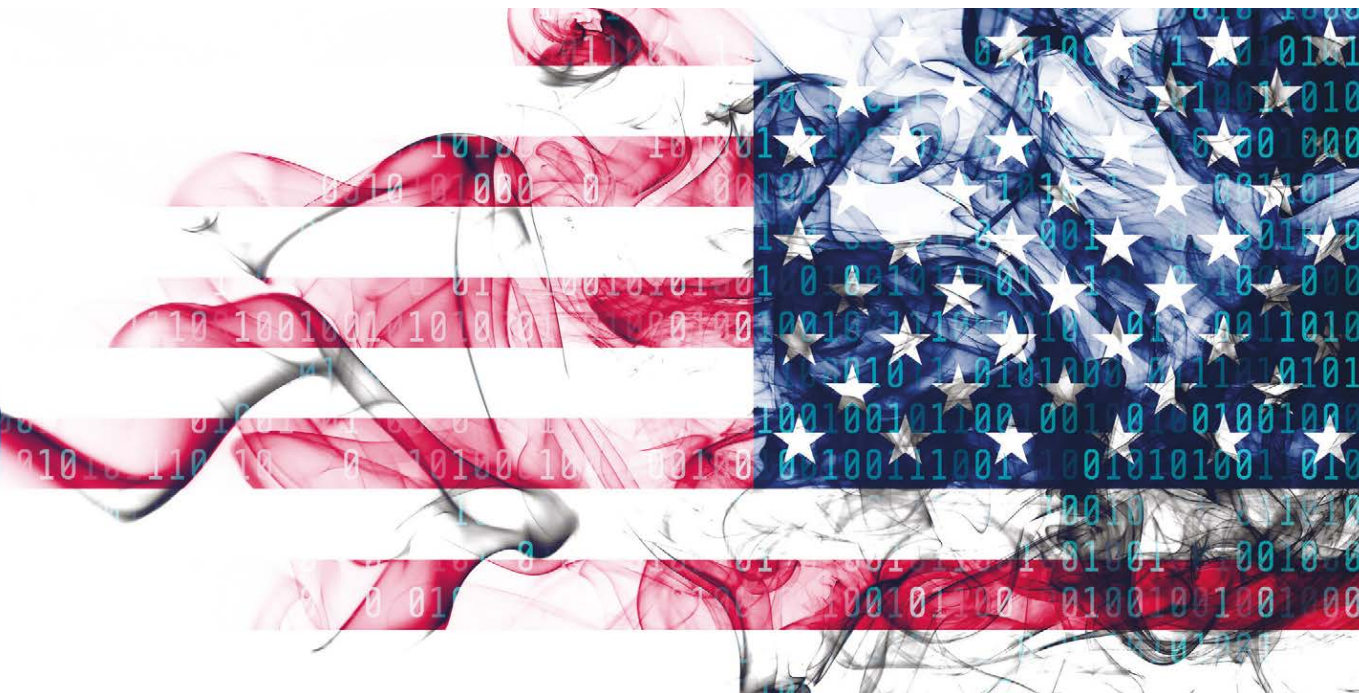
to support further transfers, and for good reason: the Schrems II ruling required data exporters to engage in a case by case enquiry regarding whether the SCCs are enough or whether additional safeguards are required (or whether the transfer should be made at all).

The response to this issue from European regulators has been the publication of new Standard Contractual Clauses. These new SCCs, or nSCCs, are likely to form the basis for data transfers to foreign countries from the EEA moving forward. Below is a brief summary of what they are,

what they do, and what companies, non-profits and other interested personal data transfers can expect in the coming months and years.

## Timelines

The nSCCs were published by the European Commission in their final form on 4th June 2021. They are now in effect, and may be used to support data transfers. Of course, many agreements now in effect are supported by the old SCCs. It would be an impossible undertaking to replace the old SCCs with the nSCCs overnight. Cognisant of this issue,



the Commission has granted a grace period of 18 months, until December 2022 to bring all agreements into full compliance, with executed nSCCs. The old SCCs may still be used in new agreements until September 2021, but it is likely most businesses will begin transitioning to the nSCCs almost immediately.

### What has changed?

The first big change is that the nSCCs are modular. They allow for all practical scenarios in which data is transferred. Specifically, there are different modules for controller-to-controller, controller-to-processor, processor-to-controller, and processor-to-processor transfers. This is welcome clarity. The old SCCs were missing two of these scenarios, resulting in awkward arrangements and applications.

The updated nSCCs also recognise that a data exporter need not be in the EEA. This is best explained by example: Corporation A transfers personal data to its processor, Corporation B, in the United States, supported by the nSCCs. When Corporation B transfers the personal

data to its subprocessor in Mexico, Corporation B can (and must) also execute the appropriate nSCCs with the Mexican subprocessor.

The nSCCs also can address the other requirements of GDPR for contracting with processors. The adequacy requirement is but one of many requirements for contracting with entities processing personal data under GDPR. The nSCCs can present controllers with an 'all-in-one' solution for contracting with their processors.

There is a greater level of specificity required regarding what data is transferred, how the data will be processed, and how the transfer will take place (ie. once or continuously).

These are just a few of the changes. It is advisable to consult your counsel for a full understanding of these important developments. Implementing the nSCCs in a compliant and operationally efficient manner will be challenging for most organisations, but there are a few things that can be done now.

First, consider building the nSCCs into your contracting process moving

forward. This need not be done right away, but September is just around the corner.

Second, understand which vendors are impacted and start to prioritise outreach. If your organisation has a data map (and it should), this would be a reasonable place to start locating your vendors. If you have yet to create a data map, your organisation's account payable is a useful resource. Third, monitor current regulations and guidance. The nSCCs are hardly the last word on this issue. We expect to see additional guidance from other EEA regulators and of course British regulators in light of Brexit. Fourth, discuss with your counsel the best approach for transfers to certain key areas including the United States. The nSCCs attempted to address some of the criticism in the Schrems II judgment concerning US surveillance practices, but it is not clear at this early stage if the nSCCs by themselves will be sufficient for US transfers.

**Christian Auty is a partner and a leader of Bryan Cave Leighton Paisner's US Global Data Privacy and Security team**





**T**he issue of systemic risk (a single ransomware event having the potential to trigger multiple claims from a domino-like disruption) is well recognised within the insurance industry and, with recent events, something that every insurer is looking to address across their global portfolios.

Significant effort and expense has been committed by third party modelling companies to aid cyber insurers' portfolios to help our understanding of the risk as well. While they're not perfect, they do provide a basis for the industry to begin to commit capital to the risk and include that in pricing models and reinsurance considerations.

Interestingly, UK businesses – often on the smaller side – have long objected to the fact that they will ever be a target for cyber criminals. Unfortunately, they have failed to see

## Stand and deliver

**Lindsey Nelson opines on the issues around cyber risk accumulation, the thorny problem of paying ransoms, and other major developments in the cyber insurance market**

that they're often the businesses that are simply caught in the cross hairs to larger, systemic events. The Microsoft Exchange vulnerability, SolarWinds and Kaseya events have all shown that to be true, as well as substantiating the fact that increasing interdependencies between outsourced vendors and supply chain partners leaves them potentially more, rather than less, exposed to cyber risk.

### **Tackling the ransom argument**

The argument that cyber insurance funds cyber crime is flawed. There is no evidence that businesses who purchase cyber insurance are more

inclined to pay a ransom demand than those without. In our experience, it's actually the opposite. Businesses without access to the appropriate experts provided under a good cyber policy to guide them through a ransomware attack and the recovery process might think they have no option but to pay an extortion demand. However, when armed with a cyber policy's proactive cyber security tools and incident response services, not only are these businesses bolstered against attacks of this kind, but they have more technical support, and therefore options, if they go on to suffer an attack.

There's no doubt that it's in the interest of cyber insurers that ransomware is tackled. There are already close connections between the industry and global law enforcement, with threat intelligence being shared and data being gathered. By using the right professionals with the right experience, we can ensure that payments are only made when absolutely necessary and that law enforcement are kept informed so they can use the intelligence gathered by cyber insurers to track and ultimately catch the perpetrators.

### Reinsuring cyber

Cyber reinsurance demand is quickly outstripping supply which ultimately leads to an increasingly selective standalone cyber market and a barrier to new market entrants in what has historically been a soft market in its more than 20 years of existence as a line of business. Between the increasing financial impact of ransomware events, remote working exposures as a result of the pandemic, and single point of failure/systemic risk events over the last few months, it's created the perfect storm for concerns around cyber threats.

From a threat landscape perspective, cyber criminals continue to see easy access points into companies providing them with profitable results due to basic minimum security requirements not being addressed both between SME and large corporate enterprises, which may have historically looked at cyber insurance as their full risk transfer solution.

In the meantime, cyber insurers are collectively working to get back into a position of profitability following severity driven ransomware attacks by ensuring that the risk is priced relative to the exposure. The market is still in the early days of a

hard market cycle, particularly in the UK, and there is no sign of rate increases abating in the short-term until there is a concerted solution from both regulatory and private sector bodies to the ransomware dilemma. Clients are likely to find their renewals look different, however for the 85 per cent of UK businesses who don't currently purchase a cyber insurance policy, they may find it more difficult to secure terms along their buying journey without basic minimum security requirements in place.

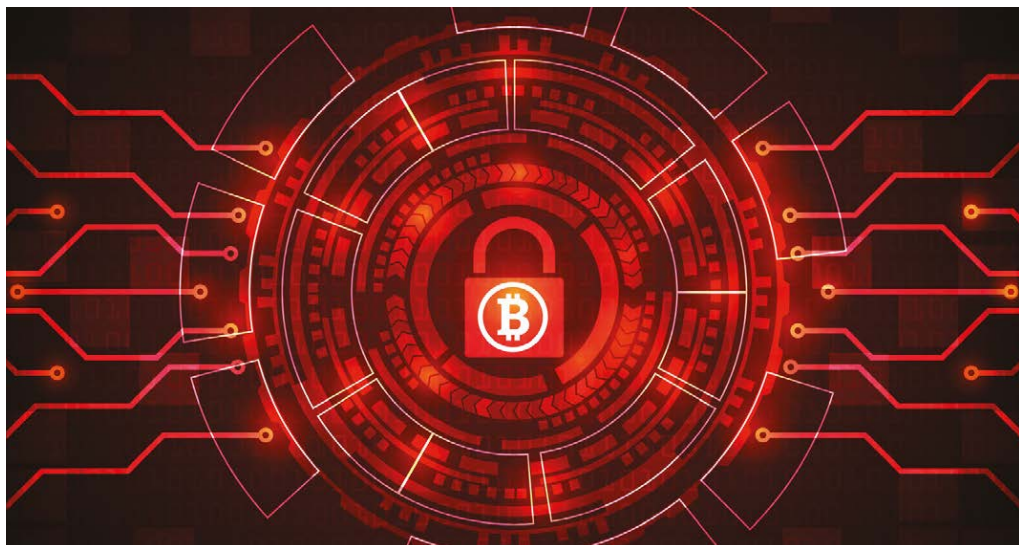
It's not all doom and gloom however. Luckily, the short-tail nature of cyber claims allows for rapid pricing feedback – and those insurers who have specialised in cyber and have the sample size and scalability across the class will be best-positioned to use that data to inform not only what stable pricing should be, but inform them on what security controls are preventing claims in the first place. Equally, never before has the cyber insurance industry been more involved in ending cyber crime – CFC, as an example, actively participate in a global Ransomware TaskForce along with the NCSC, FBI and larger

technology firms around the world. Our Cyber Threat Analysis team continue to also work regularly with the intelligence agencies around the world to gather information on extortion payments to track, and ultimately apprehend the perpetrators.

Cyber insurance is equally already evolving into something much more than coverage alone, and insurers are quickly acting to provide proactive risk management up front to prevent claims before clients even know to file one. The future and profitability of the class depends on insurers in this space also providing proactive threat intelligence, basic cyber security tools, and policyholder education. Of course, if the worst does still happen, a fast and effective in-house response can largely mitigate larger severity driven events down the line. Ultimately, we believe that a business will be at less risk as a cyber policyholder than they will be uninsured.



**Lindsey Nelson is**  
cyber development  
leader at CFC



# Political violence capital

**Demand for new sources of capital has become salient, leading many to look to the global insurance-linked securities community for support. Tom Johansmeyer writes**

The global re/insurance industry seems to be spending more and more time talking about political violence. In addition to the significant toll it can exact on communities, the implications for insurers have become increasingly noticeable. A clear upward shift in industry-wide insured losses from political violence has led to changes in risk transfer, increased insurer caution, and a salient need for better understanding.

Concern about political violence (especially riot and civil disorder) is relatively new. Re/insurers have watched terror aggregations for years, often with increasing concern, but such events have generally fallen far short of the insured losses caused by natural catastrophe events, such as hurricanes and severe convective storms. In fact, no non-terror political violence event before 2019 reached US\$1 billion in insured losses. Localised events in mature insurance markets stayed small enough to result in lower levels of insured

loss, while larger political violence events seemed to occur most often in markets that lacked sufficient insurance penetration.

The 2020 US riots have made the global re/insurance industry view political violence risk with fresh eyes. Known colloquially as the ‘George Floyd riot,’ the event generated more than US\$2 billion in industry-wide insured losses, according to PCS data. Before that, we’d recorded only 12 riot and civil disorder catastrophe events since 1950, with the 1992 riot in Los Angeles the most expensive. At US\$800 million, it was an outlier at the time, given that the average before it was less than US\$50 million.

The US event followed an even larger one in Chile the year before, with insured losses of almost US\$3 billion. At the time, re/insurers were able to perceive it as an outlier because of its size and location. Less than a year later, though, the US event showed characteristics similar to the Chilean event, suggesting an emerging trend. In both riot and

civil disorder catastrophe events, approximately one third of the insured losses came from a handful of large retailers with significant losses (fewer than five in each event).

Because of the sharp change in political violence risk, insurers have begun to respond. Some have reduced their coverage for riot and civil disorder in property programmes, and there are cases of reinsurers pushing back on certain classes of business in property treaties that don’t exclude political violence. Retail, unsurprisingly, is one of those sectors. The change may not be transformative, but there are already questions about how political violence may be covered in the future – and whether additional capacity could become necessary.

Naturally, re/insurers began to ask about ILS capacity.

The ILS community has supported re/insurers for three decades, with assets under management swelling to US\$100 billion. Despite the historical focus on natural catastrophes, ILS funds have ventured into other forms of risk, including marine and energy, cyber and aviation. Scaling standalone political violence, however, has been difficult. To find out why, PCS

**“The ‘George Floyd riot’ generated more than US\$2bn in industry-wide insured losses, and made the global re/insurance industry view political violence risk with fresh eyes”**

Event	Year	Industry loss
Colombia riot	2021	< US\$150m
‘George Floyd’ riot (US)	2020	> US\$2bn
‘Yellow vest’ protests (France)	2018-2020	€200m
Hong Kong riot	2019	US\$77m
Chile riot	2019	~US\$3bn
Colombia riot	2019	US\$50m
Bolivia riot	2019	US\$167m

Recent non-terror political violence events (Source: PCS, a Verisk business)





surveyed 15 ILS funds. Representing more than 60 per cent of the industry by AuM, they said that they could write more political violence protection, but not as it's currently being offered.

Only 20% of respondents said they have explicit constraints on political violence risk. They explained, though, that those limitations only apply to some of the funds they manage, generally accounting for less than half of AUM. As a result, such constraints should only apply to a single-digit portion of the capital represented by all of the participants in our research. However, only four of the 15 responding to PCS are either active in political violence or have been recently. One of them only assumes the risk in certain non-catastrophe specialty lines.

Two more are open to the risk, but they haven't seen transactions they'd like to participate in. A fifth said they'd look at standalone political violence trades but are sceptical about pricing being sufficient, and a sixth indicated the need for 'more sensible structures' while specifying, "It's a risk we quite like".

#### What would have to change?

At the top of the list, according to our research, are rate and structure. Fund managers told us that the opportunities brokers bring to them either don't have enough premium or are structured in a way that makes them unattractive to the ILS community. In addition to rate and structure, PCS learned that ILS funds are concerned about the ability to model non-terror political violence, a

problem that's exacerbated by having to underwrite the 'human condition'.

Seemingly remote hedges by ILS funds may not look like they have direct implications for original insureds seeking cover for political violence. One-off trades far from the risk tend to feel more like financial exercises. However, initial transactions – whatever the motivation – are crucial to the eventual development of a robust market with a consistent and reliable flow of capital. As the ILS market becomes more comfortable with political violence risk, re/insurers will gain more tools for supporting their end clients.



**Tom Johansmeyer**  
is head of PCS, Verisk

# The only way is up

**R**ecession, cyber threats and regulatory intervention continue to weigh heavy on the professional indemnity market, with availability of cover and pricing both areas of major concern for buyers. Now, a new report suggests the London PI market could be well positioned to take on the myriad challenges facing the industry.

With 94% of insurers planning to write the same or more business in the next 12 months, confidence is high and appetite strong, according to law firm, Clyde & Co's May survey of insurance professionals and buyers.

The industry acknowledges that there are three key areas where COVID-19 might change buyers' risk profiles in the next five years, the heightened threat associated with weakened supervision being the most prominent. Increased privacy, cyber and ransomware exposures brought about by remote working comes in joint second together with the financing and insolvency consequences of the crisis.

The claims environment has already begun to shift, according to the report, with a quarter (24%) of buyers have seen more PI claims brought against their organisation in the past year, while 35% report an increase in the size of claims.

Looking ahead, some 95% of insurers expect to see more PI claims over the next two years, and 67% believe they will be more severe. Almost half of buyers, meanwhile, predict more losses and a similar number expect the size of these losses to increase.

With prices continuing to harden,

**Availability of cover, COVID, pricing and claims were recently identified as the biggest problems in the hardest professional indemnity market for years. Despite this, the London Market is bullish about prospects**

underwriters see an opportunity to write more restrictive cover for higher rates.

Renewals, however, do represent a challenge, according to Clyde & Co's report. Many brokers are still working to complete placements that in previous years would have been straightforward. Likewise, only 52% of insurers anticipate that buyers will be able to maintain existing policy aggregates – 40% are not.

## Surprising and gratifying

Simon Konsta, partner, Clyde & Co comments: "These findings are both surprising and gratifying for the insurance market. That appetite is strong despite the challenges being faced should give the market a lot to think about as it confronts renewal season. Neither buyers nor carriers have any doubt that claims are set to rise, but there is broad agreement that London is well placed and has the appropriate capacity, competitive rates and robust claims functions to preserve its position as a preeminent international hub for PI risks.

"That 58% of our respondents foresee financing and insolvency consequences due to recession as a top concern should give us all pause for thought. Likewise, as our research demonstrates, buyers will need to consider whether a separate cyber insurance policy is required to ensure that appropriate cover is maintained. Finally, the threat

## PI: A changing market

- COVID-19: 68% of insurers see an increased threat associated with weakened supervision and 58% expect greater privacy, cyber and ransomware exposures associated with COVID-19
- Claims: 95% of insurers expect a greater number of claims in the next two years with 67% expecting them to be more severe
- Market appetite: 48% of insurers are planning to write the same level of business in the next 12 months with 46% expecting to write more
- Pricing: 100% of buyers and 99% of insurers expect rates to rise
- Coverage: 94% are expecting to offer more restricted cover for specific perils in the coming year and 46% to see a reduction of non-core PI covers
- Market dynamics: 83% of insurers expect market change in the form of new entrants, exits and consolidation. 39% expect more business to be written through MGAs, binders and delegated authority over the next two years.

Source: Clyde & Co

of regulatory intervention will see certain professions confronted with challenging premiums and, as a result, cover for these areas is becoming more restricted."

**Clyde & Co's Confidence in the Face of Challenge report is available at [clydeco.com](http://clydeco.com)**





# Plan ahead for the unexpected.

In a changing world, flexibility in your business continuity planning is key.

Regus Workplace Recovery, together with Pronto Recovery can offer award winning options for flexible workspace and technology recovery to keep your business up and running, whatever the crisis.

**Get in touch today**

Visit [regus.co.uk/workplace-recovery](https://regus.co.uk/workplace-recovery)  
or call **0800 279 7131**

[prontorecovery.com](https://prontorecovery.com)  
**+44 (808) 164-2790**

**Regus**<sup>™</sup>

**Pronto**  
Recovery



# Training risk champions

**IRM trainer and risk practitioner Alexander Larsen explains why risk champions are so crucial in embedding an effective enterprise risk management structure and culture into an organisation**

In order to implement an effective enterprise risk management structure in an organisation, the process, tools and procedures, along with risk knowledge, decisions and behaviours all need to be communicated and integrated at every level. A risk champion is a great option for achieving this goal.

There are numerous names and roles for a risk champion but, most commonly, they are employees in an organisation who, although their primary role may not be risk management, they are responsible for providing support within their own department or division when it comes to risk reporting.

Also known as risk coordinators, risk officers, risk management business partners and risk business partners, they are essentially an extension to the core risk management function, and can communicate risk information and influence risk culture and behaviours. In addition, they can report back to the risk management team on areas for improvement such as what frustrates staff in relation to the risk management approach, and help to overcome some of those challenges.

## **The role of the risk champion can vary but includes:**

- Providing feedback on an employee's view of risk management process
- Supporting identification and reporting of risk
- Ability to identify blockers

- Communicating the risk management vision to staff
- Acting as a subject matter expert in certain disciplines (eg. geology)
- Acting as a 'translator' between risk management and their technical department
- Building a risk aware culture within the organisation, including appropriate education
- Providing guidance to the risk manager on the best way to implement risk management in specific areas of the business and at what pace.

## **The risk champion network**

One risk champion will likely be insufficient in an organisation looking to identify risk across all its departments, and in these cases, a risk champion network offers a better reach.

It allows departments to take ownership of risk, something that may otherwise be difficult because those outside the risk management function can tend to assume the responsibility for it sits with the risk management function department. It also brings a sense of risk ownership to the front line.

The risk champion framework places the responsibility for assessment and mitigation firmly within those departments and risk owners, and having a risk champion within each department or area has often been found to enhance and strengthen ownership of the process.

International firms with a

network of offices, usually spread across countries and continents, often struggle to build a consistent risk culture. This is partly because risk management teams have limited reach, but also because different geographies and management teams – and the prevailing country or regional culture – will have different attitudes to risk. Again, in these cases, having a risk champion network can improve consistency in risk identification, understanding and reporting.

## **What kinds of roles might risk champions have in different organisations?**

You will need to develop a job description for your risk champion network. This will vary depending on the risk maturity of your organisation and how engaged, knowledgeable and conversant staff are with risk management. It could be as simple as updating departmental risks at defined intervals, or it could go further to include ensuring risks are analysed in line with the published criteria. It may be worth considering a stipulation that risk champions talk to each person in a department individually or you might ask them to run workshops.

It could be that you want the risk champions to drive risk management within their own departments, but instead of the risk champion being responsible for the risk register, they instead support their manager in maintaining it.

With the right risk champion and a structured training and development

programme, they could even drive training throughout the organisation. This tends to be correlated with the level of organisational risk maturity.

You also need to think about how much time they have and what percentage of it should be dedicated to risk management. That will dictate how much the risk management responsibility they can take on alongside other roles that they perform. Such time commitments are likely to be different in different departments, areas or regions.

Whichever approach you take, it needs to support your ultimate aim, which is to drive risk culture. Managers are responsible for departmental objectives and therefore they should also be responsible for owning the risks for their departments.

### What education do they need?

In a company with good risk maturity, your managers are more likely to suggest someone with the right blend of knowledge, competency, skills and

commitment. Otherwise, you can try to improve the process by guiding managers on the kinds of skills you need. For instance:

- Champions need to be relatively senior
- They need to have the authority and ability to speak to people at higher levels
- They need to have been in their present role for a while
- They may need a certain personality
- You might want someone with certain qualifications (eg. a financial or engineering background)
- They need the visible support of the CEO and the risk manager.

You don't want to step on managers' toes, but if you can give them a good idea of what you are looking for and how the specific characteristics and criteria will benefit them, you're more likely to get the champions you need.

Once risk champions are in place, training should begin from the outset.

### Induction and basic training

Context is important, so risk champions need to have an introduction to risk management and an understanding of their roles and expectations as they relate to the organisation.

Training should consist of communicating why the organisation is focused on risk management, the benefits of the programme, and the resources dedicated to it. It should also include the foundations of risk management: What is risk? What is risk management? How do we identify, assess and manage risk?

These sessions should be interactive and involve various identification and assessment exercises.

Running sessions that enable risk champions to work together also adds tremendous value – allowing them to build an informal relationship that can be helpful in understanding other parts of the business, and helping them to understand how risks may interconnect, eliminating bias and group think in the formative stages. It also builds a network of risk champions that can rely on each other and not always feel the need to ask questions of the risk management department.

### One-to-one training

The risk manager should be hands-on and deliver dedicated one-to-one training and support. This may take the form of shadowing, inviting champions to workshops and involving them in the preparation and running of the sessions, as well as observing them running sessions as time goes on. Essentially the role is to hand-hold until they are confident enough and providing the right quality of output to go it alone. These one-on-one sessions need to be integrated with the annual



performance review process and cycle which should also include individual development plans for risk management.

#### *Soft skills training*

Soft skills are a vital skill for any risk professional and risk champions will benefit greatly from such training, depending on the expectation set upon them. As an example, if they are expected to run workshops, then they should receive facilitation skills training, for presenting reports they should have presentation skills, and for dealing with numerous stakeholders they should be offered communication skills training.

These are just some examples of the types of soft skills training that would be extremely useful in their roles, although there are numerous others.

#### *Multi-layered and multi-year training*

Whilst the above training should be in place as standard, it is important to have a training plan in place that aligns with the longer term aspirations of the risk management department.

Linking the training to the risk maturity aspirations of the organisation might be a good way to develop the training requirements. As an example, if the expectation is that quantitative risk analysis will be a feature of the risk management process across the organisation within a three- to five-year period, it might be useful to build a training programme that prepares your risk champions to either understand the data inputs required or even go as far as training them on how to run Monte Carlo simulations with the help of software.

Having a three-year training programme (or longer) in place which guarantees a set number of days for training, for example five to ten days'

### **The Institute of Risk Management**

The IRM is the leading professional body for enterprise risk management, helping to build excellence in risk management to improve the way organisations work.

The Institute provides globally-recognised qualifications and training, publishes research and thought leadership and sets professional standards, which define the knowledge, skills and behaviours today's risk professionals need to meet the

demands of an increasingly complex and challenging business environment.

IRM members work in many roles, in all industries and across the public, private and not-for-profit sectors around the world. The Institute is independent and not-for-profit.

The full portfolio of IRM's qualifications and training courses can be viewed at: [www.theirm.org](http://www.theirm.org)

training a year over a three-year period, will greatly improve the skills and knowledge of the risk champions whilst also meeting the needs of the organisation's risk maturity aspirations. This has the positive knock-on effect of improving the overall risk culture of the organisation, with the risk champions able to better communicate the benefits of risk management to staff as well as improved support to all involved in the risk management process.

To really add value to the training programme, it can be undertaken in conjunction with an organisation such as the Institute of Risk Management, which would allow the risk champions to achieve a certificate by the end of the programme. This ensures not only top quality bespoke training developed specifically for the organisations needs and in conjunction with a highly regarded professional training and education body, but it also adds an incentive to be a risk champion, and to remain a risk champion, for those three years or whatever period the risk champions role has been specified as.

Encouraging HR to include such a certificate as a prerequisite for certain managerial promotions, and so on, will even further encourage people to

willingly put themselves forward for the role of risk champion.

#### **Typical agenda:**

When training a risk champion, the following elements should be covered;

- What is risk management?
- What does risk management look like in the world?
- What does the organisation see as risk management (focus on opportunities, too)?
- What is risk appetite and tolerance? What is the organisation's current risk appetite?
- How do we go about identifying risk?
- How do we measure those risks?
- How do we manage those risks?
- How do we communicate and what reporting requirements do we have?
- How to facilitate workshops and risk conversations.
- What tools are available for risk management?



**Alexander Larsen**  
IRM trainer and risk practitioner and president, Baldwin Global Risk Services



**CIR** Risk Management

AWARDS 2021

**The 12th annual Risk Management Awards**

**The pinnacle of achievement in risk management**

# **BOOK YOUR TABLE**

**4 NOVEMBER 2021**

**LONDON MARRIOTT HOTEL, GROSVENOR SQUARE**

**[cirmagazine.com/riskmanagementawards](http://cirmagazine.com/riskmanagementawards)**



**@CIR\_MAGAZINE #RISKMANAGEMENTAWARDS**

Headline Partner



Supported by



# The overhaul continues

**A major overhaul of UK building safety in the form of the Building Safety Bill will bring about a number of changes that insurers need to be aware of, as Kathryn Turner explains**

**T**he impending Building Safety Bill, which has been described as the biggest change to the building safety regime for 40 years, is set to pass in 2023. Drawn up in response to the Grenfell Tower fire, the Bill aims to introduce more stringent regulatory measures for high-risk buildings – those of 18 metres or six storeys or more in height

On 19th January 2021, housing secretary Robert Jenrick announced that a new national regulator was to be established to ensure that materials used to build homes are safe. The Regulator for Construction Products will have strong enforcement powers,

including the power to remove from the market any product that presents a significant safety risk; the ability to conduct its own product testing when investigating concerns; and the power to prosecute companies that flout the rules on product safety.

The RCP will operate within the Office for Product Safety and Standards and will see a shift in focus from Trading Standards, which has typically been the enforcing authority in relation to the current regulatory regime on product safety. The RCP will, however, work with Trading Standards as well as the Building Safety Regulator to encourage and enforce compliance.

## How will high risk buildings be assessed?

There will be three ‘gateways’ at key points of the construction cycle for buildings deemed high-risk. In order to pass through one gateway to the next, the BSR will require evidence that the standards of the previous gateway have been satisfied.

- Gateway 1 (at planning application stage): BSR will consult with stakeholders to assess various design matters like fire safety and water supply.
- Gateway 2 (at construction stage): This stage is designed to provide a ‘hard stop’ where construction cannot begin until the regulator is satisfied that the duty holder’s design meets safety requirements.
- Gateway 3 (at management stage): All the prescribed documents and information (Hackitt’s “golden thread” of information) must be handed over to the Accountable Person. Duty holders will also be required to submit ‘as-built’ information to the BSR.

The Building Safety Bill offers welcome guidance to the industry at a high level. In theory, a safer industry will not only keep residents safe but also eventually reduce the number of claims made by professionals and that, in turn, should lead to fewer losses.

However, the Bill also creates the new role of the ‘accountable person’, who will be responsible for assessing building safety risks on an ongoing basis and is required to submit



information to the new BSR. The BSR will have wide-ranging duties and functions, including taking over the building control regime for high-risk buildings as detailed above, enforcing sanctions for non-compliance, improving the competence of those working on such buildings and overseeing the safety of those buildings in occupation.

### What will the sanctions be?

The Bill will be the most significant regulatory reform in the construction sector for years, strengthening existing sanctions as well as introducing new ones. Prosecutions for contravention of building regulations are to be extended from two years to 10 years and the requirement to correct non-compliant work from one year to 10 years.

Additional breaches, which could result in criminal sanctions, include failing to appoint an AP or building safety manager with the necessary skills and knowledge to carry out the role; failing to register a high-risk building with the BSR before it becomes occupied; and failing to provide information to the AP.

It also covers providing false or misleading information to the BSR; obstruction of authorised officers, such as blocking the BSR from carrying out an inspection; and failing to provide information or documentation to the BSR.

Penalties include sentences of up to two years in prison, unlimited fines or both.

The BSR will be able to issue compliance notices if there has been, or is likely to be, a breach of building regulations. It will also be able to issue stop notices during the design and construction phase that require work to be halted until any serious non-compliance is addressed.

In addition, it will be obligatory

to report to the BSR any structural and fire safety occurrences that could cause a significant risk. As a result, businesses will need to put in place internal processes in order to comply with their reporting obligations.

The BSR will also have the power to appoint a 'special measures manager', replacing the AP and building safety manager as the individual in control of a high-risk building where issues have been uncovered.

Perhaps most importantly, the Bill makes it an offence for an AP for a high-risk building to disregard, without reasonable excuse, any relevant requirement which places one or more people in or about the building at critical risk. The scope of the Bill is therefore extremely wide with the possibility for prosecution being similarly broad.

### Insurance ramifications

The new legislation is, without a doubt, a positive and long-awaited step in the right direction to improving building safety and fire safety risks. Insurers have long called for fundamental reform of the building regulatory and safety system due to the number of buildings that have been left with poor levels of protection.

The changes brought about by the new legislation should mean fewer insurance claims under buildings or construction related policies due to improved building safety and reduced fire risks. Further, the preservation of the thread of information together with the mandatory reporting requirements, combined with the increased sharing of information introduced by the Bill, should assist insurers and risk surveyors in better understanding the risk they are being asked to underwrite and survey.

However, it is the creation of

the AP and the increased levels of responsibility that will now sit clearly with building owners, managers, developers, contractors and other construction professionals, together with the power of enforcement, which is likely to have the biggest impact upon the insurance sector.

The government is likely to be watching the insurance sector's response closely – particularly the extent to which professional indemnity cover is offered in respect of the new roles identified and whether any public policy decisions are required if the construction industry cannot respond to the demands placed upon it by the new regime.

Therefore, whilst the measures to improve building safety are undoubtedly important and should reduce the risk of loss and damage, consideration will need to be given to the insurance market's ability to provide adequate cover to dutyholders and construction professionals. Insurers may want to consider what changes are required in order to mitigate the added risk introduced by the Bill such as bespoke exclusions, additional questions at inception or training for risk surveyors.

The scope of appetite among insurers to cover those working on high-risk buildings, and the consequential effect on prices, remains to be seen. Either way, the management of high-risk buildings is likely to be an extraordinarily expensive, difficult and time-consuming task with a heavy weight of responsibility on duty holders, in particular the AP.



**Kathryn Turner is an associate, Crime & Regulatory at Keoghs**





# BUSINESS CONTINUITY AWARDS 2021

## 1 SEPTEMBER 2021

London Marriott Hotel  
Grosvenor Square

# SHORTLIST ANNOUNCED

The pinnacle of achievement in business continuity, security and resilience

In association with

Sponsored by

Supported by



HORIZONSCAN

RISK - RESILIENCE - READINESS



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

Regus<sup>™</sup>  
workplace  
recovery



Insurance  
Today

[businesscontinuityawards.com](https://businesscontinuityawards.com)



@CIR\_Magazine #BusinessContinuityAwards

## Hot in the city

✓ **The number of cities at extreme risk for heat stress is expected to increase by 58% from 482 today to 762 by 2050, as global warming takes hold, according to the latest research from the analysts at Verisk Maplecroft**



London is forecast to feel as hot as Milan by 2050, with the loss of productivity estimated to cost over £2 million. It is just one of a number of the world's major cities at growing risk of extreme heat stress as global warming takes further hold, according to data from Verisk Maplecroft.

Heat stress can trigger confusion, dizziness, fatigue, nausea and even death; with the strain on healthcare facilities of increasing concern for affected cities. Transport and power grids are also forecast to face disruption, with a reduction in GDP predicted as productivity and outputs fall.

Asset owners, especially those involved in real estate, will see operational and retrofitting costs soar as cooling demands increase and buildings require better heat resilience.

And corporate supply chains should expect commodity price increases, falling labour productivity and growing labour risks in warmer months.

The key word for cities, asset owners and corporates alike, according to Verisk Maplecroft, is resilience.

"Climate change is going to force a reevaluation how we live and work in urban environments, and global organisations and governments will have to start building these issues into their planning," says senior environmental analyst, Liz Hypes. "If emissions remain unchecked, temperatures and humidity will quickly rise, leaving many cities facing more frequent and

severe heatwaves."

"Heat stress will have to be front of mind in climate strategies and investment decisions from today. Failing to adapt to heat stress could have devastating effects on economies and inequalities, and turn some of the world's most important urban environments into much less hospitable places to work, live and invest."

To illustrate what the future looks like under this scenario, Verisk Maplecroft has selected a number of major cities to show how rising heat stress will change northern urban environments. The below are just a few examples.

### Turning up the heat

Intensifying levels of heat stress over the next 30 years will make Glasgow as warm as London. While Glaswegians may welcome the change from iron grey skies and rain, those familiar with London's stifling underground system will not relish the thought of heat in the UK capital feeling more like Milan does today.

Milan's July average high temperature comes in around 30°C, 11 degrees warmer than London's current average, elevating the frequency and length of rail delays as more days climb over 24°C. Yet London's transition into a climate like Milan's equates to more than just a sweaty commute. As heatwaves like London's 2019 and 2020 events become the summer norm by 2050, the city could see losses upwards of US\$2.8 billion in productivity – from increased labour inefficiency, illness and workplace injuries and delays due to impacts on transport – despite its workforce being largely staffed by people in climate-controlled offices.

Milan will be mostly buffered from the severest impacts of heat stress due to its economic focus on financials and services, but Rome's transition will be harsher as it moves into a climate more like that of Agadir, Morocco.

Italy's capital is no stranger to the effects of heat stress, but this will be amplified by 2050 when it will experience an additional 41 heat stress days per year, which occur when temperature and humidity exceed 25°C on a measure known as the Wet Bulb Globe Temperature.

The 2017 heatwave saw the Italian capital, renowned for its aqueducts and water fountains, threatening to ration water for over a million residents.

Pressures on power and water supplies, excess mortalities and labour capacity losses are already shared across Southern European cities like Lisbon, Bologna and Athens. But Verisk Maplecroft's data suggests they will, on average, transition into feeling more like Middle Eastern and North African cities over 400 miles to their south, where fatalities related to heat stress are most concentrated.

**Source: Environmental Risk Outlook 2021 from Verisk Maplecroft**



# We know our way around... Risk



We study it, research it, speak on it, share insights on it and pioneer new ways to measure it.

Covering 180 countries, we bring a proactive, flexible and fresh approach to over 100 classes of specialty insurance.

[tmhcc.com](http://tmhcc.com)



**TOKIO MARINE**  
**HCC**

Tokio Marine HCC is a trading name of HCC International Insurance Company plc (HCCII) and Tokio Marine Europe S.A. (TME), both members of the Tokio Marine HCC Group of Companies. HCCII is authorised by the UK Prudential Regulation Authority and regulated by the UK Financial Conduct Authority and Prudential Regulation Authority (No. 202655). Registered with Companies House of England and Wales No. 01575839. Registered office at 1 Aldgate, London EC3N 1 RE, UK. TME is authorised by the Luxembourg Minister of Finance and regulated by the Commissariat aux Assurances (CAA). Registered with the Registre de commerce et des sociétés, Luxembourg No. B221975. Registered office: 26, Avenue de la Liberté, L-1930, Luxembourg.



Sponsored by



TOKIO MARINE  
HCC

**CIR**  
CONTINUITY INSURANCE & RISK



► How have cyber exposures evolved in the financial sector, and how well are institutions doing when it comes to managing the risks? CIR's latest podcast with sector experts at Tokio Marine HCC covered the key issues

# Hitting the jackpot



### Cyber risk is all pervasive. How are financial institutions coping?

Xavier Marguinaud: Financial institutions were very early adopters of cyber insurance since it was developed in the US in the mid-1990s. In fact, they were the second largest buyer after the market was developed for the telecoms sector. The truth is financial institutions have always been a prime target for hackers. With the B2B, B2C duality of their business model, the sheer amount of sensitive data they are handling, and also the rather high level of digitalisation in this sector, you could even say it's a jackpot target.

According to a study released by Forbes in 2018, financial services firms fall victim to cyber security 300 times more frequently than businesses in other industries. Note that I'm referring to this sector as being often targeted, not as being especially vulnerable. In fact, this industry is rather mature, and has a good overall awareness level. Since the very beginning of its cyber journey, this industry has constantly challenged itself, complying with rigorous regulatory requirements, implementing avant-garde security, and deploying innovative solutions including cyber insurance.

I think it's important to note here that financial institutions are considered among the best-placed in being able to identify cyber threats and contain incidents. IBM's 2020 *Cost of a Data Breach* report ranked the sector as the fastest to identify and contain a breach, at 233 days, the average being 280 days.

### How has the industry evolved from a cyber risk perspective?

Jonathan Pflieger: Some large financial institutions are confronted with millions of attacks on a daily basis. Cyber risk management is a clear

# Hitting the jackpot

**How have cyber exposures evolved in the financial sector, and how well are institutions doing when it comes to managing the risks? CIR's latest podcast with sector experts at Tokio Marine HCC covered the key issues**

part of their operational resilience, and therefore a strategic priority. In recent years, cyber risk governance has improved, with clear ownership and engagements from IT to business line management, and all the way up to the board.

The sector has also made progress when it comes to cyber risk culture, as the human factor is so relevant. The industry has continued to invest heavily in IT security, systems and people, and comply with an ever-growing number of regulations and guidelines across numerous jurisdictions. The European Commission's Digital Operational Resilience Act, which will be a focus for European institutions in the coming months, illustrates this well.

Financial institutions have also improved the quantification of their cyber exposures by taking advantage of access to more risk data. Additionally, the industry has become adept at sharing threat intelligence and exchanging best practices. Regulators and governmental agencies have also taken part in some of these initiatives.

### What would you consider to be the main exposures?

Ignacio del Corral: Ransomware has been the greatest cyber threat for some time now, with attacks carried out by highly sophisticated groups. Attackers are now also threatening to disclose data to the public if the victims don't agree to pay, even going

as far as notifying the customers and regulators directly if the victims do not comply.

Supply chain attacks also pose a significant risk. Attackers target organisations that, when compromised, may serve as a stepping stone to larger, more robust companies, which are the real target of the attackers. Customers place a large amount of trust in banks to protect their data and privacy, so we have a responsibility to protect ourselves and our customers.

### What are the most commonly underestimated, or even completely overlooked exposures?

Eduard Blanxart: M&A activities are probably one of the most underestimated exposures in cyber. They usually involve very relevant and complex systems migration, and sometimes this process is mismanaged. One of the most striking cases was the TSB migration in 2018.

Testing procedures are key. Considering the integration process usually takes months, or even a year, it is also quite challenging from an underwriting perspective.

Insider threats are probably the second forgotten cyber exposure, as recently highlighted by ENISA. This is especially sensitive at this moment, as many banks worldwide are restructuring their operations, so we will probably see more incidents originating from insider threats in the next few months.



### What key underwriting elements would you take into consideration to assess the risk management maturity of an organisation in the sector?

EB: Well, I could talk for an hour about key underwriting elements! But to name a few, insurers must apply sound underwriting and risk management tools in the area of cyber underwriting, which is becoming more and more complex. Assessing supply chain risk would involve a thorough look at enterprise security architecture capability, high dependency links, or single points of failure. Legal aspects are also highly relevant in cyber. And the rise in ransomware attacks necessitate a clear protocol for dealing with that. Cyber risk is also increasingly seen as a potential systemic risk for the financial system.

### What's your perspective on the headline risk management elements?

IdC: Collaboration is key. The full ecosystem has to work together for a robust response. This includes suppliers, government, regulators and cross sector collaboration at a global level. Initiatives, such as the Financial Services Information Sharing and Analysis Centre, which promotes information sharing, play an important role. The European Financial Services Roundtable, and the World Economic Forum are also involved in valuable efforts against cyber crime, with recent support from Europol, Interpol and the ABI.

### Can you share any stories with readers that paint a picture of what can go wrong, and of how an incident might escalate?

EB: Whilst it's often the case that cyber attacks come from outside, malicious employees can pose a significant risk. In one case, a member

of a bank's staff extracted very sensitive data from the datacentre – millions of records of members and former members. This individual did not have authorised access to the data himself – he had persuaded three other employees with the relevant rights to access it.

The data was downloaded from his computer to USBs on several occasions over the course of a year, and the rogue employee had distributed the data to third parties in return for relatively nominal compensation. In my opinion, this incident could have been avoided, not only by having a stricter USB policy, with limitations on downloads, but also by incorporating behavioural detection capabilities, to analyse the behaviour of the employees. For instance, you can create alerts if an employee downloads some files in the middle of the night, or if the size of the file is too large.

### What emerging cyber risk trends should be on our radars?

EB: Affirmative and non-affirmative cyber risk exposures, or silent cyber, are a hot topic. Also, the interaction of the cyber policy with other policies such as crime policies, PI, D&O or even property damage is not so clear when a cyber incident occurs, so it's very important for insurers to be as transparent as possible, by having clear coverage, and clear, explicit exclusions. Speaking of which, insurers are now introducing some additional limitations on their policies, such as sub-limits for ransomware, full exclusions on system failures, and on migration of systems, or other types of limitations.

JP: The ongoing digitalisation of supply chains and ecosystems will continue to create new risks and broaden the attack surface of financial

institutions. In order to prevent systemic risk, financial institutions will need to continue to thoroughly assess IT controls of critical service providers, such as infrastructures or cloud service providers. I also believe that the increase of consolidation across various segments of the industry may also entail more risk, considering integration and migration of systems. The number and cost of cyber attacks is not set to decrease in the near future. Financial institutions will need to continue to invest in the technology, people and processes to keep their frontrunning position when it comes to cyber risk management.

**These are just a few highlights from this podcast, which you can listen to in full at [www.cirmagazine.com](http://www.cirmagazine.com).**

**Get in touch with Tokio Marine HCC at [www.tmhcc.com](http://www.tmhcc.com)**



**▶ Ignacio del Corral**  
Group Vice-President  
Global Head of Own Insurance  
Grupo Santander



**▶ Jonathan Pflieger**  
Underwriting Manager  
Financial Institutions  
Tokio Marine HCC



**▶ Eduard Blanxart**  
Senior Underwriter  
Financial Lines  
Tokio Marine HCC



**▶ Xavier Marguinaud**  
Head of Cyber  
Tokio Marine HCC





20 years of innovation delivered worldwide  
enterprise risk management and analytics software

any risk      any time      anywhere

:- enterprise risk manager® software  
on secure private-cloud or on-premises  
:- risk to cost & schedule analytics software  
:- Greybeard® risk & project controls consulting

riskhive.com  
ianbaker@riskhive.com  
+44 1275 542839  
+44 7818 898997



# BUSINESS CONTINUITY AWARDS 2021

## 1 SEPTEMBER 2021

London Marriott Hotel  
Grosvenor Square

# THE FINALISTS

The pinnacle of achievement in business continuity, security and resilience


In association with

Sponsored by

Supported by



[businesscontinuityawards.com](https://businesscontinuityawards.com)

 @CIR\_Magazine #BusinessContinuityAwards





# BUSINESS CONTINUITY AWARDS 2021

## Business Continuity Awards 2021 - The finalists

### Business Continuity / Resilience Manager of the Year – sponsored by ResKube

- Ann Clark, Janus Henderson Investors
- Chris Godsmark, Roche
- Tara McCarthy, Experian
- Helen Rickards, Allianz
- Jayne Romanczuk, Bupa
- Jon Seaton, Tesco Bank

### Student of the Year

Special Award – To be announced on the night

### Newcomer of the Year – sponsored by the Retail Business Continuity Association

- Emily Clemente, Castellan Solutions
- David Field, London North Eastern Railway
- Jennifer Newton, Allianz
- Georgie Stevenson, PlanB Consulting

### Adviser of the Year

- Mohinder Kainth, CyberCX
- Suneel Kumar Thakur, Boston Consulting Group
- Swapna Malepati, Cognizant Technology Solutions
- Russ Parramore, National Fire Chiefs Council

### Lifetime Achievement

Special Award – To be announced on the night

### Team of the Year – sponsored by Horizonscan

- Allianz & LV
- Bupa UK Business Continuity Team
- Coca-Cola EuroPacific Partners
- Cognizant Technology Solutions
- Dell Technologies
- DHL Supply Chain

- Experian
- Janus Henderson Investors
- Marks & Spencer
- National Fire Chiefs Council BC Mentoring Team

### Specialist Company of the Year

- B C Training
- CMAC Group
- CyberCX
- Fusion Risk Management
- Instinctif Partners
- KRTS International

### Specialist Technology Company of the Year

- F-24 UK
- Fortress Availability Services
- WhereScape

### Most Effective Recovery of the Year

- Allianz & LV
- Alan Lloyd, Daisy Corporate Services
- DHL Supply Chain
- Marks & Spencer
- Roche
- South Yorkshire Fire & Rescue

### Strategy of the Year

- Allianz & LV
- Anglian Water Services
- Coca-Cola EuroPacific Partners
- Cognizant Technology Solutions

### Strategy through Partnership

- CMAC & Home Office Immigration Enforcement
- Royal Mail & DHSC & Deloitte
- Horizonscan BCP & PD Ports





# BUSINESS CONTINUITY AWARDS 2021

## Business Continuity Awards 2021 - The finalists

### Initiative of the Year

- Kelly Services
- Marks and Spencer
- Unilever & PA Consulting
- YUDU Sentinel & Ross-on-Wye Town Council

### Incident Management Award

- Allianz
- Anglian Water
- DHL Supply Chain
- South Yorkshire Fire & Rescue

### Transformation Award

- Coca-Cola EuroPacific Partners
- Cognizant Technology Solutions
- LV Financial Services
- Roche

### Resilient Workforce Award

- Boxtree Recruitment
- DHL Supply Chain
- Financial Ombudsman Service
- LV Financial Services
- Royal Mail Group
- Tate Galleries

### Excellence in BC in the Financial Sector

- Arab National Bank
- Mastercard
- T. Rowe Price & PA Consulting

### Excellence in BC in the Retail Sector

Special Award – To be announced on the night

### Excellence in BC in Industry

- DHL Supply Chain

- Kelly Services
- Royal Mail Group

### BCM Planning Software of the Year

- Agility Recovery
- Castellan Solutions
- Crises Control
- Daisy Corporate Services
- Services Conseils RDI Inc.

### Most Innovative Product of the Year – sponsored by Regus Workplace Recovery

- Credit Passport, CRIF Realtime
- Fusion Risk Management
- Reskube, Fortress Availability Services

### Cloud-based Services

- Agility Recovery
- Databarracks
- F-24 UK
- YUDU Sentinel

### Global Award

- Abqaiq Plants-Saudi Aramco Company
- Abu Dhabi Ports
- ADCB
- Assan Aluminium
- Dubai Economy
- Kuwait Telecommunications Company
- Saudi Customs

### Best Contribution to Continuity & Resilience

- B C Training
- Daisy Corporate Services
- DHL Supply Chain
- Marks & Spencer & NaCTSO



@CIR\_magazine #BusinessContinuityAwards



Chartered  
Insurance  
Institute

Standards. Professionalism. Trust.

# Be recognised.



Corporate Chartered status is a visible sign of your commitment to professionalism and helps you attract and keep the very best talent.

**Be Chartered.**

**[www.cii.co.uk/chartered](http://www.cii.co.uk/chartered)**

# NATIONAL INSURANCE AWARDS 2021

## THE WINNERS

[nationalinsuranceawards.co.uk](https://nationalinsuranceawards.co.uk)

Brought to you by

**Insurance**  
Today

In partnership with

**CIR**  
CONTINUITY INSURANCE & RISK

Sponsored by

**idex**  
IDENTIFYING EXPERTISE

Supported by

 Chartered  
Insurance  
Institute

Showcasing outstanding performance in general insurance



# NATIONAL INSURANCE AWARDS 2021

## WINNERS 2021

### Commercial Lines Broker of the Year

WINNER: Business Choice Direct

### Claims Team of the Year

WINNER: Brit Insurance

### Commercial Lines Specialist Broker of the Year

WINNER: McCarron Coates

### Personal Lines Broker of the Year

WINNER: P J Hayman & Company

### Travel Insurance Award

WINNER: Goodtogoinsurance.com

### Claims Initiative of the Year

WINNER: Zurich Insurance & Carpe Data

### Lloyds and the London Market Award

WINNER: Munich Re Syndicate

### Cyber Product of the Year

WINNER: Kovrr

### InsurTech Award - sponsored by IDEX Consulting

WINNER: MOTIX Connected

### Commercial Lines Insurer of the Year

WINNER: Direct Commercial

### Communications Team of the Year

WINNER: AXIS Capital

### Innovative Product Award

WINNER: QOMPLX:UNDERWRITING

[nationalinsuranceawards.co.uk](http://nationalinsuranceawards.co.uk)

Brought to you by



In partnership with



Sponsored by



Supported by



@InsTodayNews #NationalInsuranceAwards

[nationalinsuranceawards.co.uk](http://nationalinsuranceawards.co.uk)

# NATIONAL 2021 INSURANCE AWARDS

## WINNERS 2021

### Innovative Product Award - Technology

WINNER: Cazana

### Initiative of the Year

WINNER: Sedgwick

### ESG Award

WINNER: Willis Towers Watson

### Specialist Coverage Award

WINNER: Paymentsshield

### Growth Company of the Year

WINNER: Lloyd & Whyte

### Insurance Recruiter of the Year

WINNER: Insure Recruitment

### Insurance Law Firm of the Year

WINNER: DAC Beachcroft

### Digital Insurance Award

WINNER: Ki Insurance

### Loss Adjusting Award

WINNER: Sedgwick

### Inclusion and Diversity Award

WINNER: Bupa

# NATIONAL 2021 INSURANCE AWARDS

[nationalinsuranceawards.co.uk](http://nationalinsuranceawards.co.uk)

Brought to you by

**Insurance**  
Today

In partnership with

**CIR**  
CONTINUITY INSURANCE & RISK

Sponsored by

**idex**  
IDENTIFYING EXPERTISE

Supported by

 Chartered  
Insurance  
Institute

[nationalinsuranceawards.co.uk](http://nationalinsuranceawards.co.uk)



@InsTodayNews #NationalInsuranceAwards

## Industry views

➤ There are numerous and clear warnings that cyber attacks are on the rise, and that attackers are launching precision strikes against firms thought likely to pay ransoms and offering weak defences.

The cyber risk landscape has become much more dangerous throughout the pandemic, with ransomware attacks hitting headlines regularly. Waves of new attacks have made for different and disturbing findings.

Companies have embraced digital transformation and employees have switched to remote working in the past year, presenting opportunities for cyber criminals to exploit weaknesses in defences. Ransomware in particular has become an epidemic of its own.

In June, the The REvil criminal gang demanded a US\$70m ransom, paid in cryptocurrency Bitcoin, in return for unlocking the files of thousands of businesses caught up in the same attack. The gang meanwhile negotiated with individual firms for smaller ransom payments. In May, DarkSide, another group of cyber criminals, managed to shut down almost half of the oil supply to America's east coast for five days, by attacking Colonial Pipeline. Authorities managed to recover the majority of a US\$4.4m ransom paid in Bitcoin after that attack.

The UK authorities have released new guidance on cyber security for large and medium-sized firms. The update, *The 10 Steps to Cyber Security*, is a collection of advice from the National Cyber Security Centre that supports chief information security officers and other security professionals to keep their company safe by breaking down the task of protecting an organisation into ten components. It is being unveiled during CYBERUK, a virtual gathering of thought leaders from the cyber security community and hosted by the NCSC.

*The 10 Steps to Cyber Security*, which were first published in 2012 and are now used by a majority of the FTSE350, have been updated to capture challenges posed by the growth of cloud services, the shift to large-scale home working, and the rise and changing nature of ransomware attacks.

The NCSC also released ransomware and malware-specific guidance in February 2020. This guidance is aimed at helping private and public sector organisations deal with the effects of

malware. Following its guidance, the NCSC said, should reduce the likelihood of becoming infected; the spread of malware throughout your organisation; and the impact of the infection.

If an organisation has already been infected with malware, including ransomware, the NCSC has a list of urgent steps to take. Smaller organisations should refer to the NCSC's Small Business Guide, and larger organisations should refer to the NCSC's Mobile Device Guidance.

A 'defence in depth' approach is a good way of keeping out ransomware attackers, and limiting the effects of any breach in security which does still occur. Risk management has plenty of tools in the armoury to help here.

Getting the right IT advice and IT security technology in place are more important than ever. Back-ups of essential data are important, like any conventional business continuity plan, although hackers' focus on publishing sensitive information means backing it up is not necessarily a useful response to such a threat.

Where the risk management professionals can also help is in the non-technology aspects to increasing security. Risks arising through employees' actions or inactions have risen in particular during the pandemic. Staff working from home, using their own laptops, or using their company machines for personal use are a major source of risk.

This makes it all the more crucial that the right governance, controls policies and procedures are in place; and that risk awareness is built up among employees through training and educational efforts about how to keep themselves and the company safer from attack.



➤ **Julia Graham is CEO of Airmic**

In association with







What's your view? Email the editor at [deborah.ritchie@cirmagazine.com](mailto:deborah.ritchie@cirmagazine.com)

For our insurance clients all around the world, 2021 has been a year of great change. Global Insurance Law Connect recently published its third *Risk Radar*, looking at trends in insurance around the world. This year, for the first time, many of the critical issues that our lawyers report in their different markets have converged, with a truly universal focus on cyber security, climate change and the impacts of the pandemic.

The pandemic put a stop to the world as we knew it. In pure claims terms, we are yet to quantify the full costs and impact because so many cases across the world are being hard fought by both sides. Some cases are settling, but not in all markets, and overall the BI cases currently in litigation will impact the insurance industry, reputationally, if not financially.

However, on the positive side, the last year has seen the opportunity for digital innovation in the insurance industry finally enacted. It is said that the first three months of lockdown accelerated the digitisation of the insurance world by five years. In country after country, we hear reports of innovations in products, customer service, and claims processes. Client service, if nothing else, has benefitted from the shifts caused by repeated lockdowns.

Yet, fast digital innovation and home working has also highlighted the vulnerability of IT systems, and the increase

in cyber risk is yet to be properly understood or measured. We must balance the risk and the reward in this growing market segment, which, in the last 15 months has globally been battered by both an increase in the number and cost of claims.

The final shared issue is climate change. In many countries, insurers have begun to work on developing new covers linked to new energy sources and adapted lifestyles. It can only be a positive if we can move from seeing climate change as a preventer, and instead see it as a catalyst for innovation, and for helping clients to manage new and different risks.

And in this environment, it is all the more important that different markets and geographies share approaches, regulatory challenges and stories of innovation. Let's work together to innovate on this critical issue for us all.



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

In association with



GLOBAL INSURANCE LAW CONNECT

The global pandemic continues to cause uncertainty for businesses, and risk managers remain at the forefront of ensuring organisations survive and adapt. There's currently a lot of focus in the UK on the risks associated with a return to the workplace, but this is only one specific aspect of the much bigger challenge of adapting to ongoing, unpredictable change.

One of the most important skills of the risk manager is their ability to connect disparate parts of the system, using often voluminous data to create insights and information about the next challenges which the business may face. This sense-making is even more critical given the magnitude of the current crisis, which could otherwise obscure the major and interconnected risks we face. Action is needed now to understand and manage the response to climate change risk, cyber risk, supply chain disruption, and the business threats from growing economic and geopolitical volatility.

Rising to this challenge goes well beyond traditional risk management approaches with its focus on risk registers and core processes. Great risk management is increasingly also about understanding horizon threats and identifying ways to build sustainable growth – whether that's new markets, global opportunities, upgrading infrastructure, or investing in new technology and automation.

By channelling their skills and attention towards learning from the current crisis in a way that identifies new sources of value and growth, professional risk managers can help bring their organisations into a new competitive league.

Excellent risk management has never been a greater priority, and to be effective it must not be about stifling innovation and risk taking, but instead about enabling rapid growth and adaptation. Professional and qualified risk managers maximise the chance of sustainable growth by optimising risk and making deliberate, informed decisions that position their organisations to respond to crises and exploit positive opportunities.

The IRM and IOR stand ready to support the global risk management community in these critical goals.



**Stephen Sidebottom is chairman of the Institute of Risk Management**

In association with



## Puzzling it out

✓ **A new whitepaper explores how the insurance industry can help shape climate policies, and outlines a number of priority areas where insurance product innovation can support climate mitigation and adaptation**

In this year of climate action, much has been said about the power of the insurance industry and its role in climate risk mitigation and adaptation.

A number of forces are shaping the demand for (and opportunity in) product innovation towards net zero across the industry, including customers, policymakers and shareholders. And now, global insurance industry group ClimateWise, convened by the University of Cambridge Institute for Sustainability Leadership, has released a whitepaper exploring the potential contribution of innovative insurance products in the transition to a net zero economy. The report draws on the expertise of ClimateWise members including Aon, Allianz, Aviva, Axa, Lloyd's, Zurich, and makes recommendations to support the insurance industry's meaningful part in the decarbonisation of the global economy.

*Product Innovation for Net-Zero Within the Insurance Sector* highlights the need for collaboration both within and beyond the sector, including active engagement with the insurance supply chain and government, in order to create an enabling landscape to drive net zero.

Lucy Stanbrough, chair of the ClimateWise managing committee and head of emerging risks, Willis Research Network at Willis Towers Watson says: "The entire insurance value chain – from modelling firms to loss adjusters, brokers to legal advisors – all hold pieces of the puzzle and innovation will be needed in all areas. I am looking forward to supporting our members accelerate action and level up understanding across the sector. From risk services that help reduce transition risks for clients, to the creation of incentives towards a lower carbon economy through the insurance products it offers to customers, the transition presents an opportunity to build a better business for the industry's clients in the future."

These drivers, alongside the expertise and influencing potential of the insurance sector to shape the agenda and policies, have informed the whitepaper's nine key priority areas for insurance product innovation to support climate mitigation and adaptation:

1. Enabling and incentivising low carbon choices
2. Mainstreaming the encouragement of climate mitigation through efficient and resilient reinstatement
3. Implementing environmentally sustainable claims servicing
4. Enabling capital flows towards green solutions through risk transfer solutions
5. Creating removal-based carbon offsets through natural

capital protection

6. Scaling emerging and existing low carbon and net-negative technologies and start-ups
7. Supporting the sustainable decommissioning of carbon-intensive assets
8. Developing risk advisory services to support clients' climate mitigation understanding and approach
9. Developing solutions for increasing climate legal liability and environmental litigation

The group proposes further recommendations to address barriers to innovation and foster greater collaboration across and beyond the insurance value chain, to support, enable and accelerate progress on this urgent agenda:

1. Expand government role: Actively engage with government on transition protection needs and private-public partnership opportunities to facilitate blended-finance approaches to scaling risk-transfer capital, such as through state-backed reinsurance pools.
2. Develop technical underwriting: Develop and scale technical approaches to underwriting based on deep-engineering expertise and close relationships with technology developers of all sizes.
3. Co-ordinate value chain: Co-ordinate the industry value-chain across brokers, insurers and others to reduce duplication through a common industry framework that recognises the unique role each player should address.
4. Drive long-termism: Drive a long-term culture that incentivises innovation and works to reduce barriers that tend to embed static business models.
5. Enhance structuring of climate data and models: Bring together model vendors and in-house analytics teams, and original equipment manufacturers to access key data sources and advise on best practice.
6. Innovate product structures: aligned to client needs, ensuring clients and customers are aware of how newer products and structures, such as usage-based products or parametrics, can benefit them.
7. Align climate and commercial priorities: so growth areas, such as IP insurance or risk consulting, appropriately integrate climate considerations in ways that enable additional innovation.

➤ **ClimateWise's report can be downloaded in full at:**  
[cisl.cam.ac.uk/climate-product-innovation-within-insurance-sector](https://cisl.cam.ac.uk/climate-product-innovation-within-insurance-sector)

# PROFESSIONAL SERVICES GUIDE

## BUSINESS CONTINUITY SOFTWARE



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

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



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

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

Shadow-Planner is based on four core modules:

- Business Impact Analysis (BIA)
- Business Continuity Planning
- Notification
- Mobile Plans

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

### How you benefit

A low-cost solution, requiring no local cap ex or hardware investments, you can:

- Get rid of inefficient, inaccurate and risky manual approaches - Word documents and spreadsheets
- Ensure all essential data (plans, contacts, documentation and more) are in a single secure location, at your fingertips
- Be assured that all data is regularly reviewed, updated and consistent
- Achieve faster ISO 22301 BC certification



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

Contact Name: Jeff Goldstein, Sales Director

Tel: +1 (203) 455-9990  
[jgoldstein@recoveryplanner.com](mailto:jgoldstein@recoveryplanner.com)  
[www.recoveryplanner.com](http://www.recoveryplanner.com)  
Linkedin: [www.linkedin.com/company/recoveryplanner.com/](http://www.linkedin.com/company/recoveryplanner.com/)  
Twitter: @RP\_BCM

### Resiliency Solutions Since 1999

#### RPX BCM Software

##### Depth, Flexibility & Scope for a Planner, Simple Enough for the Casual User

RecoveryPlanner's all-in-one RPX software brings together compliance, resiliency, operational risk and continuity to deliver a mature, integrated solution.

#### Key Features:

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

#### Continuity Consulting

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

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



## BUSINESS CONTINUITY, DISASTER RECOVERY & ALWAYS ON INFRASTRUCTURE



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

For more information:  
Call +44 (0) 344 863 3000  
Email [Enquiry.dcs@dcs.tech](mailto: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](mailto:bctenquiries@cmacgroup.co.uk)  
[www.businesscontinuitytransport.com](http://www.businesscontinuitytransport.com)  
Twitter: [https://twitter.com/](https://twitter.com/CMACgroupUK)  
CMACgroupUK  
LinkedIn: [https://www.linkedin.com/](https://www.linkedin.com/company/10540515/)  
[company/10540515/](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.



## Professional Services Guide

**To advertise in the CIR Professional Services Guide please call  
Steve Turner on +44 (0)20 7562 2434 or email [steve.turner@cirmagazine.com](mailto:steve.turner@cirmagazine.com)**

## RISK MANAGEMENT SOFTWARE SOLUTIONS



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

Contact: Phil Walden

Tel: +44 (0)1730 172020  
[sales@jcad.co.uk](mailto:sales@jcad.co.uk)  
[www.jcad.co.uk](http://www.jcad.co.uk)  
Twitter: @jcad2

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



## ORIGAMI RISK

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

Tel: 312.702.5395  
[info@origamirisk.com](mailto:info@origamirisk.com)  
[www.origamirisk.com](http://www.origamirisk.com)  
YouTube: [https://www.youtube.com/channel/UCUSGoJ\\_XoT0nz\\_K9HJXk2rQ](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.



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](mailto:keith.davies@protechtgroup.com)  
[www.protechtgroup.com](http://www.protechtgroup.com)  
LinkedIn: [au.linkedin.com/company/protecht-advisory-pty-ltd](http://au.linkedin.com/company/protecht-advisory-pty-ltd)  
Twitter: [twitter.com/Protecht\\_Risk](https://twitter.com/Protecht_Risk)  
You Tube: [www.youtube.com/user/ProtechtPtyLtd](http://www.youtube.com/user/ProtechtPtyLtd)

### The Protecht Group

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

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

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

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

## RISK MANAGEMENT SOFTWARE SOLUTIONS



**riskHive Software Solutions Ltd**  
Dilkush  
Farlers End  
Bristol  
BS48 4PG

[Rebecca.cope-lewis@riskhive.com](mailto:Rebecca.cope-lewis@riskhive.com)  
+44 7539 592 727

[Sandu.hellings@riskhive.com](mailto:Sandu.hellings@riskhive.com)  
+44 7768 866 158  
[www.riskhive.com](http://www.riskhive.com)  
Linkedin: [www.linkedin.com/company/riskhive/](http://www.linkedin.com/company/riskhive/)

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

### **riskHive Enterprise Risk Manager™**

is a secure private-cloud risk database that supports your risk management needs as they evolve. Fully configurable to meet the changing requirements of your risk management journey, riskHive ERM supports the way you want to work. [www.riskhive.com](http://www.riskhive.com)

### **riskHive Arrisca Risk Analyser**

is a stress-testing and risk analysis tool that helps you understand, evaluate and assure any Excel spreadsheet. With just a few clicks you can improve confidence in your base spreadsheet models and run Monte Carlo to underpin your decisions. [www.riskhive.com](http://www.riskhive.com)

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

**Experience. Knowledge. Capability. Expertise.**

## WORK AREA RECOVERY



### **Fortress**

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

Tel: +44 (0)20 3858 0099  
[info@fortressas.com](mailto:info@fortressas.com)  
[www.fortressas.com](http://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.

# CIR

## **CIR Software Reports**

**Advertise in CIR's next software report**

To advertise in the next CIR software report, please call Steve Turner - Telephone: 020 7562 2434 or email [steve.turner@cirmagazine.com](mailto:steve.turner@cirmagazine.com)

CIR produces three software reports a year, each updated annually, and providing the most comprehensive guide to the market's software [cirmagazine.com/cir/cirreports.php](http://cirmagazine.com/cir/cirreports.php)







Better Society  
**ENERGY  
AWARDS**  
— 2021 —

**OPEN FOR ENTRIES**

**6 October 2021**

**The Waldorf Hilton,  
London**

**Recognising the leaders of green energy**

**FREE TO ENTER - Submit your entry before the deadline and  
you'll also be entered into a prize draw for a £100 Amazon voucher!**

**Extended deadline: 20 August**

**[www.bettersociety.net/energyawards](http://www.bettersociety.net/energyawards) @CTBetterSociety #BSEnergyAwards**

Organised by:



Supported by:



A central graphic of a globe with glowing white lines connecting various points across its surface, set against a background of concentric white circles and a blue-toned cityscape at night.

**ONE Partner**  
**ONE Platform**  
**ONE View of Risk...**  
**Just when you**  
**need it most.**

Riskconnect is a global leader in integrated risk management technology and the world's largest RMIS provider. Our 500+ team members around the world have both the industry and technical know-how to understand your organisation and your challenges.

To learn what the Power of ONE can do for your organisation, visit [riskconnect.com](http://riskconnect.com).