Interview
Sarah Holland of RiskEye talks to us about social media risk

Software Report
Your guide to risk software products

Book reviews
We take a look at The RegTech Book

cirmagazine.com

January-February 2020

CIR
CONTINUITY INSURANCE & RISK

Navigating #MeToo *Employers and insurers are reassessing their risk exposure, while legislators are poised for battle*

In the shadows *The ongoing migrant crisis poses an array of potential problems for businesses, with more on the horizon*

Focus: Cyber risk *Tokio Marine HCC offers a framework for companies looking to achieve comprehensive 'cyber readiness'*

Against the world

Political risk management for an indignant age

View: "Organisations are entering an era of increased volatility with regards to workforce issues"

Comment

Our first issue of the year covers some fairly dark topics, but ones that need tackling head on, and what better time to do so? From the ugly and real-life consequences of social media to the depraved criminal activities of human trafficking rings, these murky topics are sadly relevant to businesses today. Our cover story focuses on the political risk outlook, and the risk management strategies that will be necessary to overcome them throughout what looks set to be another tense year in that regard.

A dramatic surge in protests in 2019 was experienced by a quarter of all countries, according to data from the analysts at Verisk Maplecroft, which also predicts continued turmoil in 2020 for governments ill-prepared to handle ongoing bursts of public outrage. Its quarterly Civil Unrest Index suggests that 47 jurisdictions witnessed a significant uptick in protests over the past year, particularly intense in the last quarter of 2019. An 'extreme risk' rating in the index, which measures the risks to business, reflects the highest possible threat of transport disruption, damage to company assets and physical risks to employees from violent unrest. Most sectors, ranging across mining, energy, tourism, retail and financial services, have felt the effects over the past year.

Countries rated extreme risk in the Maplecroft index jumped from 12 to 20 this year, the reasons for which are complex and diverse. In Hong Kong, protests erupted in June 2019 over a proposed bill that would have allowed the extradition of criminal suspects to mainland China; but discontent has at its roots the rollback of civil and political rights in 1997. And in Chile, protests have been driven by income inequality and high living costs but were triggered by a 30 peso increase in the price of metro tickets. Countries dropping into this category include Ethiopia, India, Lebanon, Nigeria, Pakistan and Zimbabwe. Sudan, meanwhile, has overtaken Yemen to become the highest risk country globally.

The resulting disruption to businesses, economies and investment worldwide is in the billions. In Chile, the first month of unrest alone caused the equivalent of around £3.5 billion worth of infrastructure damage, and cost the Chilean economy around £2.3 billion, or 1.1% of its GDP.

"The pent-up rage that has boiled over into street protests over the past year has caught most governments by surprise. Policymakers across the globe have mostly reacted with limited concessions and a clampdown by security forces, but without addressing the underlying causes. However, even if tackled immediately, most of the grievances are deeply entrenched and would take years to address. With this in mind, 2019 is unlikely to be a flash in the pan," the report states.

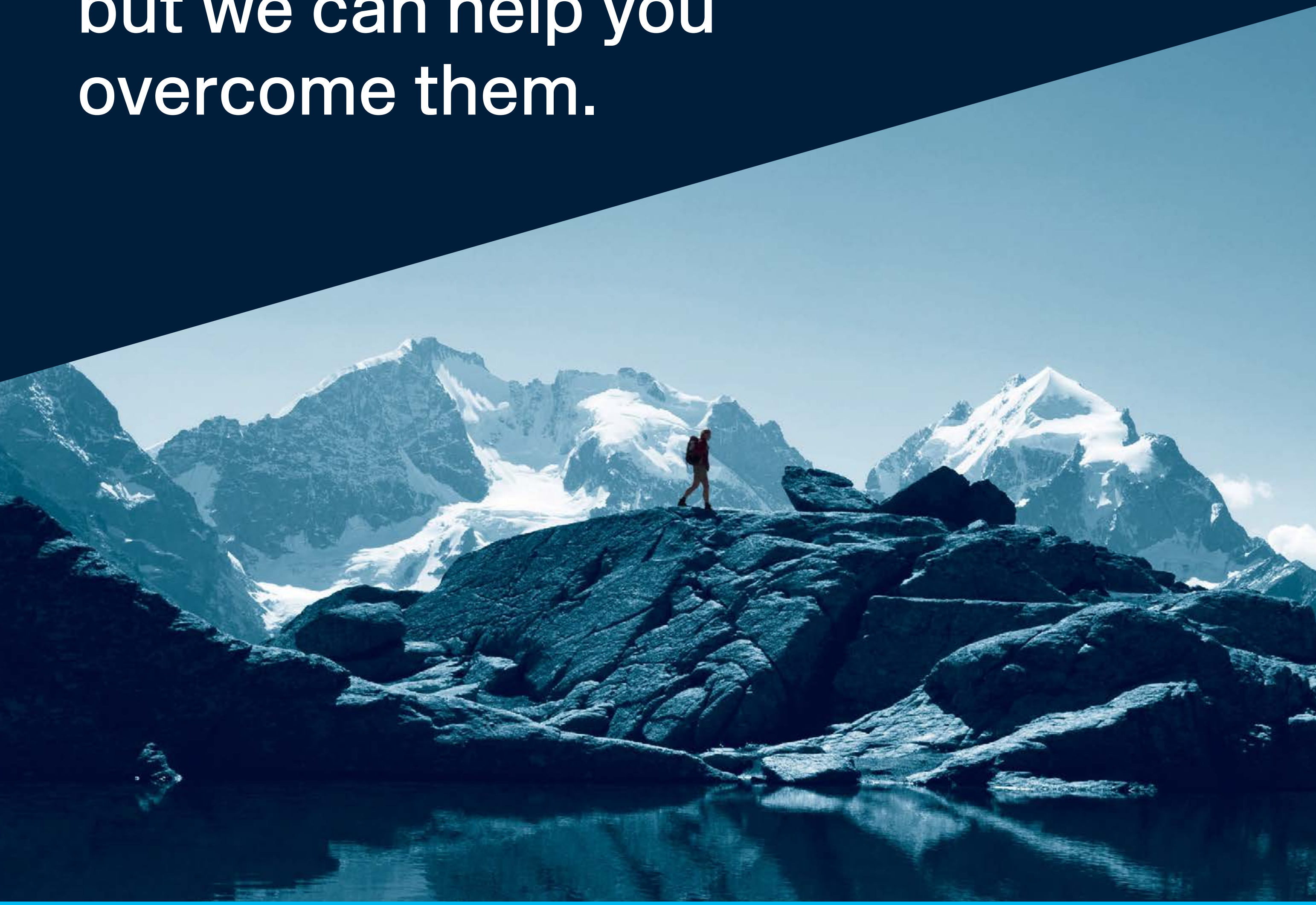
The next 12 months look likely to see more similar developments and trends, with comparable resultant losses, so companies and investors are advised to learn to adapt and live with this 'new normal'.

As I would not wish for my first column of the year to set an exclusively gloomy tone, it does look like there is light at the end of the tunnel for one of the major domestic political risk issues of the day, which has got to be good news regardless of which side of the fence you were on in 2016. And with that, a very happy new year to all our readers.

Deborah Ritchie, Editor

Crises cannot be prevented, but we can help you overcome them.

FACT24
Emergency Notification and Crisis Management



EMERGENCY NOTIFICATIONS

Whether you are assembling crisis teams or alerting all your employees – In the event of an emergency, FACT24 will notify all your stakeholders securely within seconds.

CRISIS MANAGEMENT

FACT24 is reliable and flexible during a crisis from communications and real time collaboration, through to the consolidation of auditable documents.

+2,500 customers

Listed by Gartner

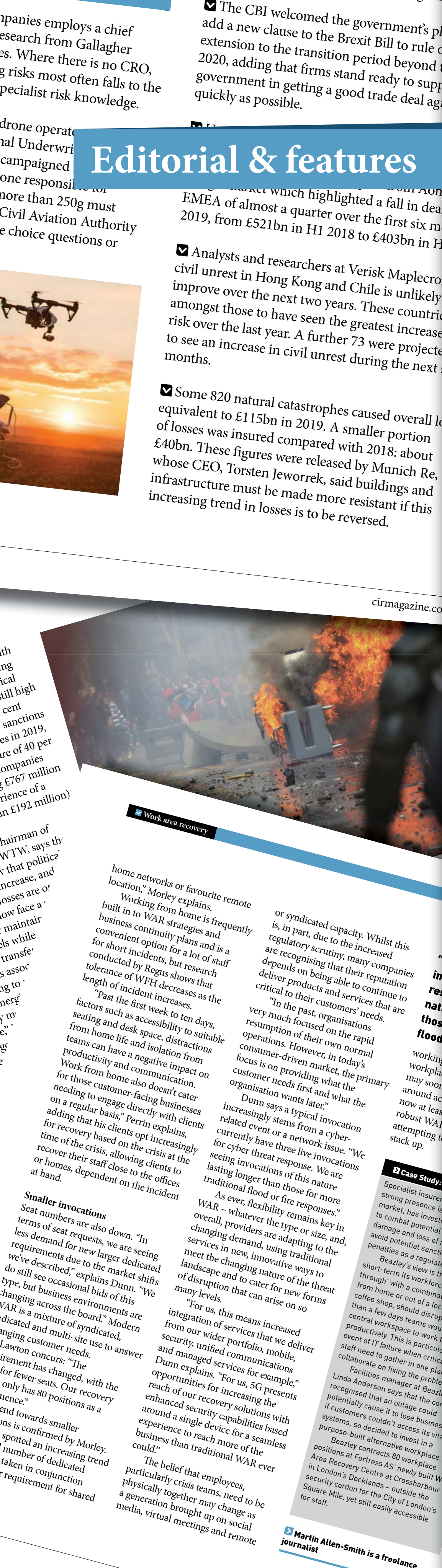
Certified by bsi. ISO/IEC 27001 Information Security Management | ISO 22301 Business Continuity Management

+180 employees

> 19 years of experience

12 locations worldwide


COVER STORY
Against the world
Political risk management for an indignant age
14



Editorial & features

News, views & regulars

Cyber readiness, key to survival

So much is said and written about cyber risks and how to prepare for them, but, as ever, the devil is in the detail. In this in-depth analysis, Xavier Marguinaud offers a framework for companies looking to achieve comprehensive 'cyber readiness'

Winners' Review

The winners of the 10th anniversary Risk Management Awards were announced at a gala dinner and ceremony hosted by comedian Zoe Lyons at the London Marriott Hotel, Grosvenor Square. Read all about it!

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

Contributing writers
David Adams
Martin Allen
Ant Gould
Joe McGrath

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

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

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

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

CIR Magazine is published by:

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

Tel: +44 (0)20 7562 2400

ISSN 1479-862X
cirmagazine.com


AVIVA

Insurers to reexamine reserving processes

A new review considers the priorities among general insurers when it comes to reserving, as well as looking at some of the other challenges they may be facing over the coming months. Deborah Ritchie reports

A large majority of general insurers are thought to be planning to review their approach to reserving over the next 12 months, both with the goal of earlier trend identification, as well as looking to ensure that all business-critical decisions are based on the latest available information.

This is according to Lane Clark & Peacock, whose recent review of the insurance market *The Future of Reserving* examines UK insurers' top reserving priorities and key challenges they face in the market.

To understand their reserving priorities and challenges, LCP met with over 80 people across 36 UK general insurers, interviewing board members, other users of the reserves and those involved in preparing the reserves, to understand their different perspectives.

"A smaller number of firms are also using or exploring individual claims reserving and alternative techniques including machine learning"

Many firms describe their ideal reserving process as having significant automation, whilst retaining human oversight of key judgements. This, the firm said, provides a 'best of both worlds' approach, and enables the reserving team to maximise time spent on value added analysis.

They are also looking for the ability to drill down into the data and analysis – focusing on the "story behind the numbers", and with a different level of detail for different users.

Head of insurance consulting at LCP, Tom Durkin, commented: "Our market review concluded that firms are ready to significantly improve benefits to the business from their reserving. It is encouraging that areas for improvement focus on specific developments which will help firms to move towards their ideal process."

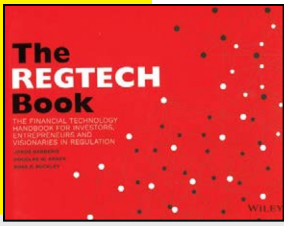
Durkin says a smaller number of firms are also using or exploring individual claims reserving and alternative techniques including machine learning. To ensure success, the firm suggests that new approaches should be focused on key business requirements, easy to use and readily explainable to the wider business.

Managing competing priorities was also revealed as the greatest barrier to change, with 75% of firms saying this is preventing them from enhancing their reserving processes. Overcoming this short-term barrier will enable insurers to build a lasting reserving process that ultimately saves time. Other key barriers include data availability.

"Our report comes at a time that reserving is high on firms' agendas," Durkin adds. "This follows the Prudential Regulation Authority publishing its 2020 priorities for general insurers in its Dear CEO letter last month, which raised a number of concerns around firms' reserving processes. The PRA has made clear that it expects these issues to be examined at board level."

By Deborah Ritchie

Inspiration for resilience professionals



The Regtech Book

Edited by Janos Barberis, Douglas W. Arner, Ross P. Buckley, Wiley, 2019.
Reviewed by Deborah Ritchie, editor, CIR
wiley.com

This self-styled financial technology handbook for "investors, entrepreneurs and visionaries in regulation" is a treasure trove of facts, figures and ideas for a sector that could be said to be at a turning point.

In an increasingly fragmented market, regulators will come under growing pressure to adapt and to collaborate with industry participants in understanding how data is collected and processed.

The marriage of technology and finance is evolving continuously. Regtech's real potential lies in its capacity to enable the real time monitoring of financial markets, something the UK's financial watchdogs recently stated as an area of increased focus.

The Financial Conduct Authority and the Bank of England detailed plans earlier this month to develop their data and analytics capabilities. The new data strategy outlines the FCA's increased focus on the use of advanced analytics and automation techniques aimed at deepening the regulator's understanding of how markets function and helping it to efficiently predict, monitor and respond to firm and market issues.

This is one of the publisher's multi-contributor handbooks, compiled with the guidance of three editors – each experts in their fields. Douglas W. Arner is the Kerry Holdings Professor in Law at the University of Hong Kong and one of the world's leading authorities on the intersection between finance, technology and regulation. He has advised on financial sector regulatory issues in markets across Africa, Asia, Australia, Europe and North America, with governments, international organisations including the Asian Development Bank and the Alliance for Financial Inclusion, and private sector institutions. He's published 15 books and over 150 articles, chapters and papers on related subjects. Ross P. Buckley, meanwhile, is the KPMG Law – King & Wood Mallesons Professor of Disruptive Innovation, and a Scientia Professor, at UNSW Sydney. His research focus is on fintech, regtech and blockchain. He also chairs the Digital Finance Advisory Panel of the Australian Securities and Investments Commission, and consults regularly to the Asian Development Bank, having also worked with government departments in 10 countries, including Australia and the US. He has twice been a Fulbright Scholar, at Yale and Duke. And Janos Barberis founded FinTech HK, a thought leadership platform, and the SuperCharger – a FinTech

Accelerator that strategically leverages on Hong Kong as a gateway to Asia. At the same time, he sits on the advisory board of the World Economic Forum's FinTech Committee and is a PhD Candidate at Hong Kong University Law School.

Their book's numerous chapters cover compliance, the age of regtech disruption, financial crime prevention, tackling regulation with innovation, Islamic regtech and regtech quality. Anti-money laundering, fintech startups and banking supervision, the regtech landscape from a regulator's perspective, blockchain and AI and digital trust protocols are also covered in depth. The handbook also tackles market surveillance, the topics of protecting consumers and enabling innovation – all familiar themes of the moment for a book of this kind. But this handbook goes further, to consider the use of regtech outside of finance, considering social purpose and impact.

"Regtech's real potential lies in its capacity to enable the real time monitoring of financial markets, something the UK's financial watchdogs recently stated as an area of increased focus"

There are any number of areas I could drill down into, but since it is timely, I'll take EU Passporting. "There is factual evidence," the book reads, "that every EU financial services authority applies its own interpretation when it comes to defining 'to provide any or all of the investment services', which leaves many financial investment firms very confused as to the meaning, and in doubt whether they are required to have a passport into an EU host member state, resulting in unnecessary additional regulatory compliance oversight and potential missed business opportunities." If that is not a compelling reason to take a look at what *The RegTech Book* has to offer, then perhaps the chapter, *The potential of regtech in improving the effectiveness of environmental regulation* or *I regulate, therefore I am? Regulating humans' and machines' conduct and culture* may pique your interest.

News briefing

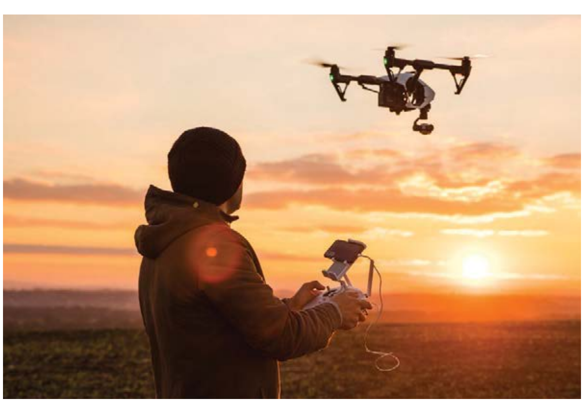
A round-up of the latest industry news

Finance and insurance firms invested the most on cyber security to 2019, at an average of £22,050 – a 23% increase on the previous year. This is according to figures from Specops, which show that businesses in health/social care/social work spent the second highest amount (£16,800) on cyber security – a staggering 506% rise on the year before.

The International Underwriting Association said that the deployment of 5G wireless networks is likely to be the single biggest technological change for society over the next few years, because it will lay the foundations for so many other new developments – from communication using 3D holograms to augmented reality glasses. Whilst exciting, it warned the associated risks and exposures are numerous and complex.

Just one in five UK companies employs a chief risk officer, according to research from Gallagher amongst 250 UK businesses. Where there is no CRO, responsibility for managing risks most often falls to the CEO, despite their lack of specialist risk knowledge.

New safety measures for drone operators were welcomed by the International Underwriting Association, which has long campaigned for change in UAV regulation. Now, anyone responsible for operating a drone weighing more than 250g must register their details with the Civil Aviation Authority and answer a series of multiple choice questions or face a fine of £1,000.



The adoption of fully automated shipping could take decades, not years. This is according to a poll conducted by law firm, Kennedy's among 6,000 people, including industry leaders in the transport and insurance sectors. Fewer than one fifth of UK respondents said that they were comfortable with the idea of autonomous vessels. Only Hong Kong is less supportive of automated vessels.

Three quarters of SMEs in the UK and Ireland said they believe their businesses can help tackle climate change, according to research conducted by Close Brothers. Some 94% of senior decision makers said they have policies in place to reduce their impact on the environment. The most popular steps include recycling, being energy efficient and going paperless.

The CBI welcomed the government's plans to add a new clause to the Brexit Bill to rule out any extension to the transition period beyond the end of 2020, adding that firms stand ready to support the government in getting a good trade deal agreed as quickly as possible.

Uptake of M&A insurance across EMEA rose over the last 18 months, despite a fall in overall deal activity in the region. So said a joint report from Aon and Mergermarket which highlighted a fall in deal value in EMEA of almost a quarter over the first six months of 2019, from £521bn in H1 2018 to £403bn in H1 2019.

Analysts and researchers at Verisk Maplecroft said civil unrest in Hong Kong and Chile is unlikely to improve over the next two years. These countries are amongst those to have seen the greatest increases in risk over the last year. A further 73 were projected to see an increase in civil unrest during the next six months.

Some 820 natural catastrophes caused overall losses equivalent to £115bn in 2019. A smaller portion of losses was insured compared with 2018: about £40bn. These figures were released by Munich Re, whose CEO, Torsten Jeworrek, said buildings and infrastructure must be made more resistant if this increasing trend in losses is to be reversed.

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

Cambridge University suggested the value of GDP at risk from commodity price shocks, extreme weather, power outages and pandemics has risen. It said that as much as £443bn (or 1.55% of GDP) could be wiped off the global economy by catastrophic events in 2020.

The problems plaguing foreign exchange firm Travelex reflect a trend among cyber criminals to deploy ransomware attacks. So said cyber analysts at CyberCube, which said such attacks could become so widespread they could stifle economic growth.

Research from Frost & Sullivan was published, predicting that an influx of established aerospace, automotive and technology companies into the urban air mobility market, backed by technological advancements and government initiatives, will drive the market for air taxis. It said the Middle East may see the first air taxi operations, as early as 2022. It expects the global market to grow at a CAGR of 46% to reach 430,000 units in operation by 2040.

The Financial Conduct Authority and the Bank of England detailed plans to develop their data and analytics capabilities, upping its focus on the use of automation techniques to better understand how the markets are functioning.

The Chartered Insurance Institute responded by saying that data alone won't prevent future consumer detriment. "Digital breadcrumbs can't replace the knowledge gained by speaking," the CII said.

The already high risk of oil supply disruption in the Middle East rose further on the back of Iranian attacks on US assets in Iraq. Several rockets were fired with the Pentagon confirming that two US assets were targeted in retaliation for the recent killing of Qasem Soleimani.

A major report published in January called for collaboration between leaders, businesses and policymakers if threats to the climate, environment, public health and technology systems are to be tackled. The World Economic Forum's *Global Risks Report* points to growing economic and political polarisation as the greatest short-term risk, and one that is leading to an "unsettled unilateral world of great power rivalries".

Those tensions in the Middle East will lead to insurers and reinsurers imposing "draconian conditions" in policies and raising rates "exponentially" in the coming months, according to DWF. That all UK flagged ships in the Strait of Hormuz are being escorted by UK navy vessels has done little to restore the status quo in the region, or confidence among politicians or businesses with assets there, the law firm said, adding that insurers and reinsurers in hull, war, piracy, terrorism, cargo and construction may raise premiums, renegotiate terms of cover and introduce riders and endorsements.

Editorial credit: Lilium GmbH

Antisocial media

Have we reached a point where social media is completely out of control? Deborah Ritchie speaks to Sarah Holland about the issues surrounding social media risk and online behaviour

Bad news has always travelled fast, but today it travels at lightning speed. And it doesn't even need to be based on facts. Social media is awash with alternatives to the truth and even has other ideas about reality. Combine this development with a growing number of internet users, and set it against a backdrop of societal unrest and political tensions, and you're left with a lawless mess.

In a few years' time, we will look back and wonder how we ever let it get so bad that politics and democracy itself could be bypassed by Twitter, or that children could be subjected to such horrific online bullying that they are driven to suicide. Meantime, stakeholders face the job of fixing social media, and taking a good look at how behaviour online is overseen.

At the less sickening end of the scale, the risks that social media presents to companies are evolving too. Who could have predicted that a mattress company might issue a warning in its IPO filing relating to the financial risk that social media influencers could pose? That they might subject the brand and the company to regulatory investigations, class action lawsuits, liability, fines or other penalties? The influencer marketing industry is thought to be worth over £6 billion. A partnership with Kylie Jenner will get your brand message to over 150 million Instagram followers. But partner companies can't control everything influencers post. RiskEye's Sarah Holland likens social media to fire – used well, it can be a powerful tool; but let it get out of hand and it is very likely to burn you.

Behaviour online has reached a point where anything goes, with sometimes devastating consequences for individuals, particularly young or vulnerable people. With governments slow to tackle the problem, this now seems to have reached fever pitch. How has social media risk changed for companies?

People now rely upon the internet for information. Of course, we still tune into the TV, but we are very quickly moving into a world where soundbites and quick, easily digestible information are the favoured source. And people largely believe what they see online.

But online is not being policed or protected, and there are no boundaries or limits to what can be said or inferred, and there is no sense of what the truth is any more. Think back to the recent UK and US elections. How can people make an informed decision when they don't know what they are reading is correct or true? And how can companies truly understand what they are dealing with? How can they tell if it is one of their competitors behind that malicious comment? How can you operate optimally without knowing?

It feels like we don't know how to behave online, and at the same time, there is no overarching accountability. All of this is contributing to what we at RiskEye refer to as a 'truth emergency'.

For many organisations, this also plays into their number one risk of what is said or published online about them. Online reputational risks, while published in the virtual world, can actually translate into real life consequences for companies and for people.

Platforms like GlassDoor profess to inform prospective employees better than other recruitment sites because the reviews are produced by the 'employees'. Verification of an account with any email address, means anyone can sign up and create reviews, whether genuine or not. The anonymous nature of their 'service' allows anyone to say anything about any company. These supposed former employees may not even have set foot in the building – there is no policing of it whatsoever. And there is no platform for defence, so the representation is completely skewed. It is the same with Google reviews – anonymity drives bad behaviour. Both of these companies are highly driven by advertising revenue, and have limited or weak standards. So the reviewed can simply be hung out to dry – judged 'guilty' by social media.

"Perhaps it is time to replace the antiquated BBC licence with something that is more fitting for our modern age – something that identifies and licenses users to operate, cooperate and contribute online in a way that they would be proud to put their name to"

Sarah Holland, chief operating officer, RiskEye

What are the most successful organisations doing to safeguard their value?
I'm often told by companies that they have the problem covered as they have a public relations team.

We don't usually advise going down the public relations route in the first instance. From our perspective, we would engage PR if a problem has snowballed.

The easiest way to avoid a problem is to be proactive in avoiding the risks. You're much more likely to be successful here if you have someone expert dedicated to it – whether that's in-house or through an external consultant.

One company doing great things in this space is Heineken. It has been able to show that it has recognised all of the overarching principles of an effective social media risk management strategy and has put all the active measures in place that give them eyes on the conversation. It has an absolute understanding about what is being said online. Companies are leaving themselves unprepared and exposed to risk. If you take a look at the annual company report of any company, 99 per cent will have nothing in the area of reputation protection. Heineken is one of the few companies that has documented processes and practices in place to cover off this risk.

What impact can a crisis managed badly online have on shareholder value?
Of all the many scandals Facebook has been involved in, it was the Cambridge Analytica scandal that wiped the most off the value of the company. Some 10 per cent in fact. That's a huge game changer – people's lives, their pensions…Facebook has been embroiled in many scandals that have hit it hard. One of its most recent, uncovered by Channel 4 *Dispatches*, revealed shoddy moderation practices that at best contradicted commitment to its users and at worst ensured damaging and dangerous content could remain on the platform. This scandal knocked 10 per cent off their share price in one day. That is the equivalent of US$14 billion!

Of course, Facebook can bounce back from it as its so big, but if that's not possible, and it's too much for a small company to bear. In fact 14 per cent of companies won't recover from it.

How can social media and technology companies be held to account for the material published and shared on their platforms? Is an online licencing programme a workable solution?
Media and technology companies take little to no responsibility for what goes online. They may say that they try to ensure that nothing unsavoury is being posted, but they are not currently held to the same account as a publishing house is, and they should be.

There needs to be in place the same frameworks and governance as the traditional print industry is subject to.

Perhaps it is time to replace the antiquated BBC licence with something that is more fitting for our modern age – something that identifies and licenses users to operate, cooperate and contribute online in a way that they would be proud to put their name to. That would remove 50 per cent of the diatribe straight away. Then you cannot have a Russian bot or a disgruntled former employee pulling companies through the bushes. Such a system could also stop minors from going to dangerous websites, and could be digitally linked to national cyber security centres.

There are currently thought to be almost 4.48 billion people on the internet, encompassing 58 per cent of the global population. This number is growing every year, so as long as the internet giants are allowed to operate under their own terms, companies and individuals will be at risk online.

Interview by Deborah Ritchie

Against the world

Political risk levels increased considerably last year – with uncertainty and volatility set to continue as 2020 unfolds. Ant Gould reports on the some of the current hotspots and issues and considers the necessary risk management strategies

- The rise of populism, political violence and trade wars around the world have together placed political risk firmly on the risk management agenda.
- Companies are reporting greater political risk losses – with political violence, trade sanctions or import/export embargoes all cited as reasons.
- QBE's recent Unpredictability Index shows that almost half of UK executives cite political uncertainty as the biggest risk facing their businesses.

The recent escalation of tensions between Iran and the US following the assassination of Iranian military commander Qasem Soleimani may have dominated the headlines at the turn of the year, but it is the rise of populism, political violence and trade wars around the world – often in established and not just emerging markets – that has resulted in pushing political risk up the wider risk management agenda.

According to a study of 41 major corporations by insurance broker Willis Towers Watson, 28 suffered a political risk loss in 2019 – with a further 61 per cent of the view that political risk levels increased over the year.

Perhaps not surprisingly, against a backdrop of international sanctions against Russia, Iran and Venezuela, a US trade war with China, and the impact of Brexit in Europe, disruption of international trade was cited as the most significant risk in the majority of regions, with 58 per cent naming trade sanctions as a concern for their operations in Europe – underlining the shift from emerging to established economies. The corresponding figures were 67 per cent in Asia-Pacific, and 77 per cent for Russia and The Commonwealth of Independent States.

Concerns about political violence were also high, particularly in Africa (74 per cent) and the Middle East (71 per cent), with firms quoting increasing fears from new technologies – such as drone strikes (and less sophisticated drones than that used to murder Soleimani) – that could further exacerbate such risks.

Last year also saw an increase in the proportion of companies

reporting political risk losses, with 54 per cent of respondents having experienced a loss due to political violence, compared with a – still high – 48 per cent in 2018; 46 per cent reported losses due to trade sanctions or import/export embargoes in 2019, compared with 2018's figure of 40 per cent; and 32 per cent of companies with revenues exceeding £767 million reported previous experience of a catastrophic (more than £192 million) political risk loss.

Paul Davidson, chairman of financial solutions, WTW, says the figures clearly show that political risk continues to increase, and that related financial losses are on the rise. "Corporations now face a strategic choice to either maintain their global business models while accepting, mitigating or transferring the political risks associated with them, or attempting to realign themselves with the emerging shape of a new and apparently more nationalist global landscape," he added.

The good news, from a risk management point of view, is that the vast majority of respondents (71 per cent) said they had seen an increase in emphasis on political risk management at their company – and nearly 40 per cent were feeling pressure from investors regarding political risk management.

Companies taking part in the survey also listed their top concerns, which included US-China strategic competition, Middle East regional stability, and an 'ESG shock'. This latter risk had not appeared among the top ten in 2018, but panellists said that rising tensions between business and society were increasingly leading to political risk events.

Close to home

Looking at the wider political risk landscape, the first much-discussed area of concern – and one very close to home – is Brexit. Despite the Conservative government's considerable majority and anticipated deal – the transition process itself, is still expected to have some degree of impact on UK businesses.

Insurer QBE's Unpredictability Index, released ahead of the UK's General Election in December, showed almost half (45 per cent) of UK executives believed political uncertainty to be the biggest risk facing their businesses in the future, compared with only 33 per cent of European business leaders. The study highlights the degree of Brexit-related disruption felt by British businesses, with executives' concerns about political instability heightened for the next 12 months.

Europe in the grip of uncertainty

The implications of the UK's exit from the European Union come at a time of major potential de-stabilisation across Europe, including the appointment of new presidents of the European Commission (Ursula von der Leyen), the European Central Bank (Christine Lagarde), and European Council (Charles Michel). In addition, the stabilising powerhouse at the heart of Europe, German Chancellor Angela Merkel may well step down early, ahead of Germany's autumn 2021 general election, leaving the EU with a leadership vacuum.

And Germany is not alone as populism across France and Italy is seeing the traditional parties becoming increasingly fragmented. At least 11 countries in Europe had populist parties in government, according to a report from broker Aon last year, whilst populist parties hold on average 22 per cent of vote share across 33 European countries.

Aon's *Risk Maps*, produced with Continuum Economics and The Risk Advisory Group, also points out that where populist policies lead to greater

barriers to trade. This has increased the prospect of politically motivated moves to frustrate established contracts, while forcing firms to consider their international supply chains as tariffs and trade barriers rise.

Another by-product of populism can be anti-immigrant sentiment, which can further fuel far-right terrorism and social tension.

These issues are creating new risks for businesses operating overseas, from the security of employees and property in the face of increasing terrorism risk, to impacts on supply chains and investments as a result of populist government policies.

"Reactionary populism in the political mainstream in several countries has given extremist fringes a sense of opportunity upon which to mobilise violent protests and intimidation around divisive political themes," surmises Henry Wilkinson, head of intelligence and analysis at the Risk Advisory Group. "Far right terrorism remains a largely disorganised but growing threat. Businesses in Europe cannot be complacent about violent risks in traditionally stable markets. A comprehensive capability to monitor, assess and manage violent risks is as essential as a violent risk transfer strategy."

Looking forward, Ben May, director of global macroeconomic research at Oxford Economics, which works with specialist consultants at Control Risks, believes the EU's resilience will be severely tested in 2020. "Coalitions have become larger and more unwieldy as a result of growing political fragmentation, while attempts to keep populist and far-right parties out of government are forcing ideologically distinct parties into awkward collaboration.

"The rise of anti-establishment parties and the proliferation of more heterogeneous, less cohesive coalitions mean governments have less room to co-ordinate actions at the EU level. If they're not held hostage by individual coalition members, many are fearful that acting in the long-term interest of the bloc – which may differ from

short-term domestic priorities – will see them punished at the ballot box. Co-operation on economic issues such as fiscal policy and monetary union finds scant support in these circumstances.

"For business, the risk is that this instability and prolonged indecision will fail to convince international markets that Europe is on top of its economic and political challenges. If markets lose confidence and start doubting the stability of the Eurozone again, access to capital could become a challenge, with the result that companies whose financial fundamentals are not strong could suffer."

US policy implications

The winds of change across Europe are being fanned by wider issues, notably a strategic rivalry between two of Europe and the UK's key trading partners – the US and China – in the form of trade wars and technological competition. And despite the impending signing of a phase one trade deal by US President Donald Trump with China in January, US policy volatility will remain a concern as it could have a material impact not only on businesses trading directly with the US but with countries whose own economies could be affected.

John Minor, US national practice leader, political risk at Aon, says the idea of 'trade wars' is unsettling to business leaders and that uncertainty about the future of trade relationships – how contracts will be impacted, implications to supply chain and a business's overall ability to market in certain geographies – means decision-making is much more difficult.

"Political risks can manifest in many ways. An escalating trade war, for example, could increase the cost of completing a project or contract costs to the point of making it uneconomic, or force a company to rethink key elements of its supply chain. In the most extreme circumstances, a trade war could force some companies out of business," he says.

US political uncertainty looks set to continue in 2020. As May at Oxford Economics says: "The country is in throes of the 2020 presidential election campaign and the impeachment process. Both political exercises will be protracted, controversial and tense. Confidence in US political institutions – including the belief in the sanctity of the electoral process – is being undermined amid intense partisan pressure and external threats."

Outside of the US, tension in Iran and Iraq and across the Middle East also continues to provide political uncertainty – particularly in the wake of the US assassination in January. Outside of fears of retaliation by the Iran regime – either directly or via proxy forces around the world – there is also the threat of a blockade in the Strait of Hormuz, a key channel for the supply of oil and gas from the Middle East to the rest of the world. This increases the risk of oil and gas companies – and the businesses they supply – of being hit by severe supply chain disruption.

Assessing and valuing political risk is not easy

Risk managers trying to stay ahead of, understand and mitigate against both existing and potential political risks face a daunting challenge. However, there has been a growth in the political risk consulting and private security industries – often linked to insurance services – enabling a more diagnostic approach to modelling exposure. Examples include WTW/Oxford Analytica's political risk modelling system VAPOR and Aon's political risk monitor, Portfolio Manager, to name just two. These services mean that rather than just adding a risk premium to the rate of return of foreign operations, risk managers can increasingly make use of sophisticated scenario and simulation analysis.

Companies however differ significantly in their approaches to political risk management decision-making. Many locate responsibility for political risk in a centralised function such as security or enterprise risk management, whilst others leave responsibility with country managers.

Being armed with the right intelligence is step one; but then what? Some businesses may simply try to avoid known hot spots. For example, one oil and gas sector company told WTW that it was undertaking a major strategic shift in its geographic exposure, driven by the desire to operate in "more predictable, less corrupt and more transparent markets".

Political risk insurance

Then there is always political risk insurance, typically purchased by multinational corporations, importers and exporters, project lenders, financial institutions and capital markets, foreign investors, and contractors in industries like construction and engineering.

As says Sarah Taylor, head of political risk and structured credit at Aon, says: "Businesses operating in territories where political risk is elevated should be considering insurance that covers against government decisions that can lead to contract cancellation, when measures are introduced to create barriers to trade, and against government action that curtails business operations and/or investments."

Types of political risk losses experienced	2019	2018
Political violence or forced abandonment	54 per cent	48 per cent
Currency transfer restrictions or inconvertibility	50 per cent	58 per cent
Trade sanctions or import/export embargo	46 per cent	40 per cent
Expropriation or creeping expropriation	29 per cent	25 per cent
Sovereign non-payment	7 per cent	18 per cent

Source: Willis Towers Watson

Many companies have traditionally shied away from political risk insurance and purchased a mixture of political violence and/or property terrorism insurance. The standalone political violence insurance market – covering property damage and business interruption caused by political violence – has evolved in recent years to cover losses where there is no property damage, such as loss of attraction and denial of access. However, political risk insurance spans any potential gaps and can include expropriation, forced abandonment, divestiture, currency incontrovertibly, non-payment and contract frustration.

As awareness of political risk, and demand for insurance solutions have increased hand in hand, the political risk insurance market has grown, with cover available from a growing number of Lloyd's market players and the larger insurers. Coverage is also expanding in terms of both perils and geography, and wordings are becoming ever-broader.

Insurers are increasingly investing in stronger analytical teams and more data. However, whilst cover has expanded the range of potentially catastrophic risks has also risen, and insurers are understandably increasingly focused on who they are insuring, and their overall attitude to risk, as much as what they are insuring.

In an uncertain world, with 2020 looking to be the same if not even more unstable, political risk is coming out of the shadows. Political uncertainty is also now not just something for companies operating in, or with supply chains in, emerging markets, but has spread into established and seemingly stable economies. Against this background, it is increasingly essential for companies to assess the potential impact of the breadth of political risks they face, as well as the systemic nature of these risks and possible knock-on effects, which often reach far beyond the originating country or sector. And whilst insurance is not a panacea for every risk, the increasing availability or sophisticated analytic tools and broader insurance coverage provides risk managers with more options than ever before.

Ant Gould is a freelance journalist

Navigating the #MeToo movement

As the world wakes up to the prevalence of sexual harassment in the workplace, employers and insurers are reassessing their risk exposure, while legislators are focused on drawing up new rules around workplace behaviour. Joe McGrath writes

- As governments and legislators respond to the #MeToo scandal, employers and insurers face major challenges in how it is both defined and handled.
- Numerous companies have realised that they need to take a far more proactive approach to stamping out bad behaviour – or face the reprisals.
- Employers must also consider myriad allegations that may arise out of a harassment claim, such as accusations of negligent hiring policies.

Recent years have seen global companies increasingly focussed on implementing policies to protect their workforce by preventing sexual harassment and work-based assaults. These initiatives have not been an organic development in human resources policy. Instead, they are partly a response to the #MeToo and #TimesUp movements which revealed the alarming prevalence of harassment, predatory behaviour and sexual assault in the workplace.

Court cases relating to the highest profile cases continue to play out in the world's media at the time of writing – among the most well-known, the numerous allegations of rape and predatory sexual assault against former influential film producer Harvey Weinstein in October 2017, including one count of rape in 2013 and inappropriate sexual behaviour towards a second woman in 2006.

The emergence of these allegations would later lead to some of the world's best-known actresses coming together on social media urging others to use the hashtag #MeToo if they had ever been harassed or assaulted at work. Such celebrity names as Jennifer Lawrence, Uma Thurman and Gwyneth Paltrow gave the campaign the impetus to reach a global audience and thousands of cases in other industries began to emerge.

The movements have been devastating for some companies, which have realised that they need to take a far more proactive approach to stamping out bad behaviour – or face the reputational and legal reprisals. This has manifested in various ways across different geographies. The last two years have seen a notable rise in sexual harassment complaints globally, impacting both large and small companies in nearly every industry.

Sexual harassment charges filed with the US Equal Employment Opportunity Commission, for example, increased nearly 14 per cent in 2018 from the previous year as the #MeToo momentum gathered pace, with the federal regulator recovering US$70 million (£54 million) for these claimants, according to The National Law Review.

Kate Palmer, associate director of advisory at employment law firm, Peninsula said a failure by employers to address the changing attitudes towards sexual misconduct could have a number of far-reaching implications for firms.

"Poor control of these issues can easily cause productivity issues with a workforce and, potentially, lead to valuable members of staff leaving their roles entirely," she explains. "Increased awareness also places employers at more risk of facing a tribunal claim as a result of this. They may also find it difficult to attract talent if it has built up a poor reputation in this regard."

Assessing the cost

Beyond sexual harassment, employers must also consider myriad allegations that often arise out of a sexual harassment claim. Claims of retaliation are common, while an employee may also accuse employers of negligent hiring or creating a work culture that allowed harassment to flourish.

As governments and legislators respond to the #MeToo scandal – albeit with varying degrees of vigour – employers and insurers may face major regulatory changes that alter how sexual misconduct is both defined and handled.

In the UK, these social movements have not led to an immediate change in the law, the government appears to be readying itself for additional

legislation. Following the conclusion in October 2019 of its consultation on sexual harassment, it is weighing up potential changes, including extending the time employees are given to take a harassment, discrimination or victimisation claim to an Employment Tribunal, and strengthening the law to protect staff from harassment by clients, customers, and other third parties people from outside their organisation.

"While we wait for the government to respond to this, they have confirmed upcoming legislation that will prohibit any provision in confidentiality clauses or NDAs preventing disclosures of harassment to the police," Palmer says.

Across the pond, around 15 states, including New York, Oregon and New Jersey, have introduced new laws to help protect employees from sexual harassment and gendered discrimination at work since the #MeToo movement. The revised policies include extending the statutes of limitations to report cases of harassment, amending the arbitrary standard that harassment must be 'severe' or 'pervasive' to constitute a hostile work environment, and requiring anti-harassment training in all workplaces.

In addition, New York state passed legislation in 2018 that generally prohibits confidentiality provisions in sexual harassment settlements – a move that is widely expected to lead to a significant rise in claim rates.

With the slogan "20 by 2020", influential advocacy group the National Women's Law Center is using its weight to force more states to pass legislation over the next year. The recent revelation that the aforementioned Weinstein has reached a tentative US$25 million settlement agreement with dozens of his alleged victims – and the revelation these settlements would largely be paid off by the shamed mogul's insurers – also highlights the direct impact #MeToo is having on employers' insurance policies and ability to get adequate coverage.

Jared Zola, a partner at Philadelphia-based law firm, Blank Rome, says while he hasn't seen a notable rise in the number of claims made under employment practice liability insurance – the main cover for sexual harassment in the workplace – the actual size of the claims have increased since #MeToo as alleged victims seek greater sums to compensate for wrongdoings.

"The size of EPL claims have definitely increased over the last two years. From my point of view, getting claims paid has been more difficult. A lot of insurers are being hit hard from the property side, such as natural disaster claims, and then you have all the threat of sexual harassment claims," Zola notes.

How big is the problem?

According to the December 2019 EPL insurance market survey by Betterley Risk Consultants – which polled over 30 of the world's largest insurance companies including AIG, Hiscox, The Hartford and Travelers – insurers have hiked up their EPL rates by as much as 10 per cent over recent months as the force of #MeToo heightens.

"It's a clear indication (to us, anyway) of how hard the #MeToo increase in claims is hitting some insurers, and of the increasing frustration with harassment," Betterley notes.

#MeToo also threatens to trigger a whole new wave of directors' and officers' claims.

This impending threat first materialised at end of 2017 when, in one of the biggest shareholder derivative settlements recorded, 21st Century Fox agreed to a US$90 million (£69 million) settlement, funded by its D&O insurers, after investors alleged the company's management allowed a culture of sexual and racial harassment to pervade the company. The investors argued that this culture resulted in both reputational and financial damage to the firm.

In this #MeToo era, companies and insurers are exposed to a range of possible D&O-related claims including a failure to monitor harassment, breach of duty and allegations of ignoring or enabling harassment.

The D&O market is certainly showing signs of strain. Data from Cornerstone Research revealed that the average D&O settlement amount in 2018 was US$64.9 million (£49.9 million) – more than triple the figure from 2017.

D&O rates have also jumped up considerably the past few years, with commentators blaming an increase in securities class actions as well as

D&O trends to watch in 2020

The array of risks facing directors and officers, as well as the resultant insurance claims scenarios, has increased significantly in recent years. Allianz Global Corporate & Specialty recently highlighted a number of developments which will impact cover over the course of 2020 and beyond.

"AGCS continues to see more claims against directors and officers emanating from 'bad news' events not necessarily related to financial results," says Shanil Williams, global head of financial lines at AGCS. "Scenarios include product problems, man-made disasters, environmental disasters, corruption and cyber attacks." These types of event-driven cases often result in significant securities or derivative claims from shareholders after the bad news causes a fall in share price or a regulatory investigation. Of the top 100 US securities fraud settlements ever, 59% are event-driven. There has also been a spike in claims resulting from the #MeToo movement, where it is alleged [directors and officers] allowed a toxic culture to take hold and endure within companies. Other prevalent types of events are cyber incidents. AGCS has seen a number of securities class actions, derivative actions and regulatory investigations and fines, including from the EU's General Data Protection Regulation, in the last year, and expects an acceleration in 2020.

Failure to disclose climate change risks will increasingly result in litigation in future. Climate change cases have already been brought in at least 28 countries around the world to date with three-quarters of those cases filed in the US. There are an increasing number of cases alleging that companies have failed to adjust business practices in line with changing climate conditions. Environmental, social and governance (ESG) failings can cause brand values to plummet. "Directors will be held responsible for how ESG issues and climate change are addressed at a corporate level," says Williams. "Increasingly, they will have to consider the impact of these when looking at strategy, governance, risk management and financial reporting."

Securities class actions are growing globally as legal environments evolve. AGCS has seen increasing receptivity of governments around the world to collective redress and class actions, particularly across Europe but also in other territories such as Thailand and Saudi Arabia. At the same time the level of filing activity in the US has been at record highs in recent years with over 400 filings in both 2017 and 2018, almost double the average number of the preceding two decades. This increased activity is impacting both US and foreign companies which have securities listed directly in the US.

Alongside law firm, Clyde & Co, AGCS has compiled a risk map which assesses the risk of a company being subject to a securities group action in a particular jurisdiction, taking into account the availability and prevalence of third party litigation funding, which is regarded as a strong factor in increased group action activity around the globe. While countries such as the US, Canada and Australia see the highest activity and most developed securities class action mechanisms, overall, such mechanisms are developing and strengthening around the world with the Netherlands, Germany, England and Wales showing notable development and increased activity in recent years.

AGCS expects to see increased insolvencies which may potentially translate into D&O claims. "Political challenges, including significant elections, Brexit and trade wars, could create the need for risk planning for boards, including revisiting currency strategy, merger and acquisition planning and supply chain and sourcing decisions based on tariffs. Poor decision-making may also result in claims from stakeholders," says Williams.

All of these mega trends are further fuelled by litigation funding now becoming a global investment class, attracting investors hurt by years of low interest rates searching for higher returns.

Litigation funding reduces many of the entrance cost barriers for individuals wanting to seek compensation, although there is much debate around the remuneration model of this business. Recently, many of the largest litigation funders have set up in Europe. Although the US accounts for roughly 40% of the market, followed by Australia and the UK, other areas are opening up, such as recent authorisations for litigation funding for arbitration cases in Singapore and Hong Kong. India and parts of the Middle East are predicted to be future hotspots.

Although it is estimated around US$15bn worth of premiums are collected annually for D&O insurance the profitability of the sector has been challenged in recent years due to increasing competition, growth in the number of lawsuits and rising claims frequency and severity. AGCS has seen double digit growth in the number of claims it has received over the past five years.

Insurers are facing more legal costs due to increasing activity, as well as more settlements and claims. Another issue is that "event-driven" litigation results in aggregation issues where multiple policies may be triggered. One event could trigger both D&O and either aviation, environmental, construction, product recall or cyber insurance policy claims, for example.

"D&O insurance addresses the intrinsic strategic risks of corporations and their senior management, and over the past year the D&O market has seen major change and likely will experience further volatility in 2020," says Williams. "One of the best defences to protect against such volatility is for risk managers and their D&Os to maintain an open dialogue with underwriters and brokers, so that all parties can gain a better understanding of the risk culture and governance within an organisation."

Source: Directors and Officers' Insurance Insights 2020, AGCS

'event-driven' litigation spurred by movements such as #MeToo.

Figures from insurance broker Marsh showed D&O rates for its FTSE 100 clients increase by as much as 77 per cent in the third quarter of 2019, while for private companies, the increases were as much as 42 per cent.

David Blades, associate director of industry research and analytics at credit ratings agency, AM Best, said insurers are increasingly looking for employers to enhance their policies and procedures and overall risk controls as a consequence of #MeToo.

Joe McGrath is a freelance journalist

In the shadows

The ongoing migrant crisis poses an array of potential problems for international businesses. Addressing weak links in a supply chain – and the looming additional threat of climate change migration – may require new approaches, writes Martin Allen

- It may get fewer column inches, but problems relating to mass migration have in fact intensified as human trafficking operations up their game.
- Of particular concern for businesses are stowaway and labour exploitation risks stemming from migrants travelling along three major flows.
- By ensuring compliance and demonstrating commitment to tackling modern slavery, companies are able to reduce exposures in supply chains.

While the topic of mass migration has been bumped off the front pages by the Brexit saga, the issue – and its considerable, wide-ranging impact – has most certainly not gone away. If anything, the complexity of the issue has broadened as unscrupulous human trafficking operations looking to exploit vulnerable people become increasingly sophisticated.

The Institute of Risk Management warns that businesses need to be cognisant of all aspects of their working practices and aware of every link in the supply chain and the impact if something goes wrong. The UK's Modern Slavery Act 2015 includes a transparency and reporting clause requiring larger organisations to make an annual slavery and human trafficking report setting out what they do to "ensure that slavery and human trafficking is not taking place in any of its supply chains, and in any part of its own business".

It may be generally assumed that only the food and agricultural industries carry the risk of exploitation in their supply chains but there have also been instances in retail – particularly clothing, where huge well-known companies have been shown to have been using child labour at the root of the supply chain. Clearly this has major implications for brand perception and reputation and, interestingly, two historic cases focused on companies preaching good CSR practices in their advertising.

An increase in migrant stowaways and labour exploitation are among the key challenges threatening global supply chains, according to a report by the British Standards Institution. Its most recent Screen study highlights migration as one of a number of major threats to supply chains currently facing businesses.

Jim Yarbrough, global intelligence programme manager at BSI, says shifts in supply chain risk are being driven by dramatic changes in the geopolitical landscape. "The concern is that as supply chains change – with Chinese companies moving operations to Africa, for example, or the US sourcing goods from other South-East Asian nations – major implications will also evolve.

"Increased exposure to labour exploitation, terrorism, corruption and natural disasters must be a consideration for companies making changes to their supply chain, and best practices must be maintained in order to prevent threats to business continuity or corporate social responsibility."

As conflict, together with political and economic conditions, continue to drive mass migration, businesses have to contend with the double-edged challenge of security and corporate social responsibility risks. The BSI report records an increase in stowaway and labour exploitation risks stemming from migrants travelling along three major flows: Central to North America; Intra-South-East Asia; and Africa and the Middle East to Europe.

BSI has also flagged some regression in countries such as Brazil, where budget cuts are reducing the resources available to carry out inspections which could increase the risk of migrant labour exploitation. It says that around half all CSR incidents recorded by BSI in 2018 involved migrants. The often desperate need for income to support family leads many vulnerable individuals into labour exploitation and compels companies to invest in a more thorough understanding of their supply chain to truly assess the risk of migrant labourer exploitation.

In particular, there are some key areas to focus on in addressing some of the potential weak links in the chain. Dependency on third-party recruitment firms for contract workers or temporary workers can increase company exposure to forced labour and/or workers subject to exploitative working conditions. The charging of recruitment fees in particular puts migrant workers at risk of debt bondage. Document retention – the withholding of passports – is another red flag. In addition, working with third-party suppliers or subcontractors that are not regulated by the same standards (such as the employment of unregulated, informal labour at a higher risk of non-payment of wages or excessive working hours) is also a big risk factor.

A focus on existing migration patterns is one thing, but the picture could be about to get even more complicated. Direct threats from higher temperatures, more frequent droughts, floods and storms, and water scarcity are well-documented as the primary effects of climate change. Less heralded is how these events drive modern slavery risks, both in countries where the effects of climate change are expected to be most severe and in less directly threatened countries in Europe and North America. By the middle of this century, there could be over 140 million climate migrants, mostly from Sub-Saharan Africa, South Asia and Latin America as a combination of tougher growing conditions, poverty, erratic food prices, and conflicts over scarce resources forces people from their homes.

Sustainability non-profit organisation, Forum for the Future – which last year published <2°C Futures, a report looking at what climate resilience might look like for businesses in 2040 – sees a requirement for existing supply chains to be 'reimagined' in a more sustainable way if some of these risks are to be averted. It highlights the need for sustainable supply chains to forge ways of creating and distributing goods that get turned into products that people need, in a way that builds social and environmental capital across the producer communities.

It uses the terms 'value chains' or 'value networks' to describe this new take on the commercial, one-way nature of 'supply', encouraging businesses to recognise the contributions of all parties to their operations, adding that truly 'valued' chains have the potential to tie the world together at a time when it risks fragmenting.

"It is calculated that, by the middle of this century, there could be over 140 million climate migrants"

Will Dawson, associate director for climate and energy at Forum for the Future, points out that when it comes to climate change responses, businesses tend to focus on what is easily quantified such as temperature change and rainfall. But he adds, in doing so, business leaders can miss out numerous interconnected and powerful forces that can combine rapidly and unpredictably to create unseen problems and opportunities. "Decision-makers would do better to consider quantitative factors affecting their business's future alongside richer, multi-factor qualitative scenarios, which research like <2°C Futures affords. Being closer to the whole picture, they will be able to better understand and test their business strategy, operating models and supply chains, while also being able to identify and take action on the risks and opportunities ahead of them."

While slavery affects all sectors, industry risk data from Maplecroft shows the food and beverage, agriculture and seafood, construction, manufacturing and transport industries are most exposed to the practice. These sectors also face a perfect storm of rising interest from investors, NGOs and consumers in their social and climate policies alongside the global expansion of modern slavery laws and mandatory reporting legislation.

Sofia Nazalya, senior human rights analyst at Verisk Maplecroft, says that companies can mitigate the increased risk of slavery and forced labour entering supply chains by carrying out human rights due diligence including direct stakeholder engagement, disclosing modern slavery risks identified in their operations and supply chains, and developing standards and initiatives within the wider industry in collaboration with other businesses, vendors and partners.

She adds: "The European migrant crisis is not the only event to have exacerbated modern slavery risks. As the number of climate migrants surge, so too will modern slavery risks. Best practice measures for addressing modern slavery and climate change together includes aligning approaches to business policies, strategy, systems, supplier codes of practice, KPIs and training programmes, helping to raise awareness of social and environmental issues. It's also important to integrate both issues into responsible or sustainable sourcing programmes – businesses should map the operations of their suppliers and subsidiaries, including those working within climate-sensitive regions, where environmental and social policies are inadequately implemented."

Businesses are also urged to set up audit programmes for the highest risk areas identified in mapping exercises, and collaborate with industry peers, suppliers, governments, NGOs and other local partners to share knowledge, good practice and on-the-ground projects.

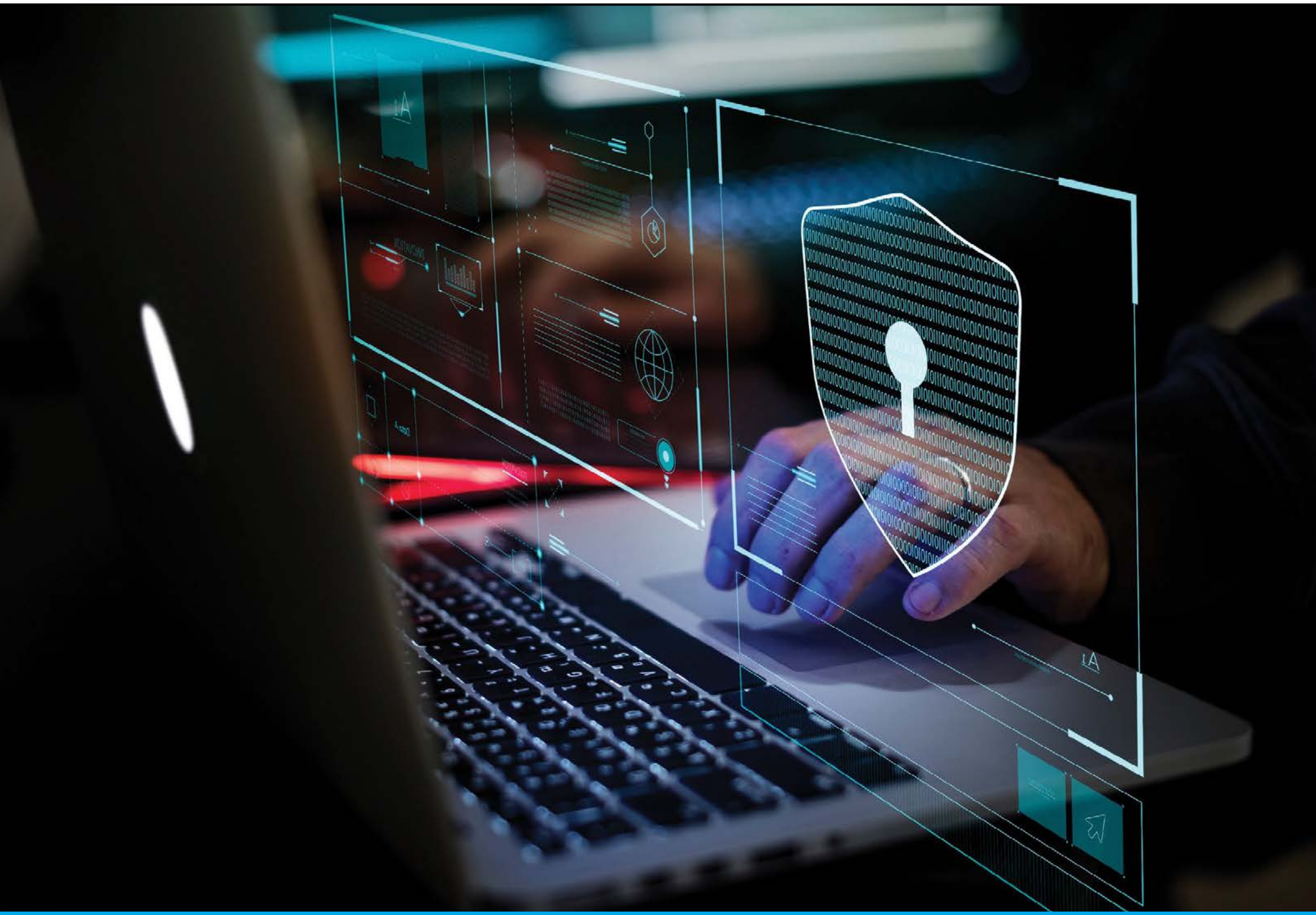
Nazalya says: "By ensuring strict compliance and demonstrating commitment to tackling modern slavery and forced labour, companies are able to reduce the risk of direct or indirect links to human trafficking in their supply chains."

Martin Allen is a freelance journalist

Sponsored by

TOKIO MARINE HCC

CIR
CONTINUITY INSURANCE & RISK



The good, the bad and the ugly *- Cyber attacks and data security have long been a growing issue for organisations and society as a whole, and with the pace of technological change, it's a problem that's about to get a great deal bigger. Deborah Ritchie reports* *p26*

Cyber readiness, key to survival *- So much is said and written about cyber risks and how to prepare for them, but, as ever, the devil is in the detail. In this in-depth analysis, Xavier Marguinaud offers a framework for companies looking to achieve comprehensive 'cyber readiness'* *p28*

Cyber risk

TOKIO MARINE HCC

Sponsored by

The good, the bad and the ugly

Cyber attacks and data security have long been a growing issue for organisations and society as a whole, and with the pace of technological change, it's a problem that's about to get a great deal bigger. Deborah Ritchie reports

Digital connectivity is now crucial both for business innovation and individual prosperity, but each creation, each step towards positive change is met with a corresponding cyber threat – that now ever-present, inescapable obstacle to doing business in the vast majority of sectors.

From data breaches and identity theft to the disruption of operations and critical infrastructure, the threats are varied and many, presenting organisations with an ongoing challenge when it comes to prevention or recovery.

Indeed, 2019 was the year the public "woke up" to the potential of its personal data, according to Information Commissioner Elizabeth Denham, hailing an "unprecedented" year for the authority, with record-setting fines and a record number of people raising data protection concerns.

In data management and security, the biggest moment of the year was as we are all painfully aware, the arrival of the General Data Protection Regulation. This, she said, saw people realise the potential of their personal data, leading to greater awareness of the role of the regulator when their data rights aren't being respected. "The doubling of concerns raised with our office reflects that," Denham said.

Since May 2018, all the European data protection authorities received a combined 90,000 breach notifications. The ten most serious GDPR breaches in the UK this year led to a total £345 million in fines, with the three highest penalties making up almost 90 per cent of the total. British Airways, Marriott International and Google were among the high-profile companies to be caught out.

Since then, Dixons Carphone has been hit with the maximum possible fine after malicious software was installed on 5,390 tills in branches of its Currys PC World and Dixons Travel chains in an event that affected at least 14 million people. And, just as its staff were returning to their desks early in the New Year, Travelex was forced to take down its website after a suspected ransomware attack. In this instance, it seems that no customer data was compromised, but the company's website had been taken offline for some time before BAU was restored.

"A civil liberties group plans to submit a legal complaint on behalf of over 1,000 people, which may set the stage for proposals contained with the Representative Action Directive"

The problems plaguing the foreign exchange firm reflect a trend among cyber criminals to deploy ransomware attacks, according to cyber analytics firm, CyberCube, which warns that such attacks could become so widespread they may stifle economic growth. Client services manager at the firm, Nick Beecroft said: "What's happened to Travelex is part of a rapidly growing trend. Ransomware has become more than a cottage industry with ransomware developers and hackers teaming up to attack companies and then divide the spoils. There are also so-called 'big game hunters' who work alone and target firms able to pay large ransoms." Beecroft also points to a movement towards the publication of 'shaming sites', with companies infected being listed.

This increasingly prevalent form of malware joins a host of other threat vectors such as phishing, denial of service attacks and session hijacking, that will keep information security professionals in business for some time to come, with new strains, such as the recent trojan malware Emotet, evolving all the time.

The World Economic Forum's *Global Risks Report 2020,* ranks cyber attacks as the second most concerning risk for doing business globally over the next 10 years. Published at the beginning of this year, the WEF report goes on to cite "information infrastructure breakdown" as the sixth most impactful risk in the years until 2030.

Both sets of respondents to the organisation's *Global Risks Perception Survey* (the multistakeholder community and the Global Shapers) identify cyber-related issues, such as cyber attacks and data fraud or theft, within the list of top 10 long-term risks.

The possibilities are endless

Already, technology is ushering in a new era of possibilities, as what was once just science fiction is quickly becoming reality. Quantum computing, AI and 5G networks are creating as many threats as they are opportunities, and lack of a global governance framework for technology risks could deter economic growth and aggravate geopolitical rivalries.

The WEF points to the need for coordination amongst stakeholders in developing solutions to this growing challenge – a challenge that will manifest substantially in AI in particular.

According to the UN's International Telecommunication Union, it will take "massive interdisciplinary collaboration" to unlock AI's potential. Security, verification, deepfake videos (the modification of images, video and audio recordings through AI so that they appear genuine), mass surveillance and advanced weaponry present problems of an as yet undefined magnitude.

Law firm DAC Beachcroft goes as far as to say AI is about to usher in a new era of offensive cyber attacks as well as defensive cyber security measures, in what may quickly become a new arms race.

"Deepfakes...could pave the way for more personalised scams and frauds," says partner and head of cyber and data risk at the firm, Hans Allnutt.

"Many cyber attacks begin with a phishing email – maliciously fooling individuals into disclosing credentials or authorising payments through emails that are surprisingly convincing. If hackers are able to utilise the sophisticated technology behind deepfakes, it is conceivable that they could mimic human voice commands by telephone so they appear to come from a trusted source."

Those companies with the impetus and resources to access this technology may fare best in this new arms race, he adds; those that do not, risk becoming the new "low hanging fruit" for attackers.

The firm's *Informed Insurance* report also foresees further and more significant enforcement action – with big name IT providers possibly in the firing line.

"The GDPR introduces direct obligations on data processors (the party who processes personal data only on the instructions of the data controller). Although fewer and fewer companies' operations fall under processor activity, due to the narrow definition applied by the ICO in the UK and more and more sophisticated uses of data by service providers, the new liability which attaches directly to data processors means that in certain circumstances they can be sued directly by data subjects and fined directly by the ICO for data breaches.

"Data regulators across Europe may soon bear their teeth and impose monetary penalties for a full range of breaches"

"With many IT providers having much deeper pockets than their clients, we consider it possible that we will see a big name IT provider at the forefront of an enforcement action very soon," Allnutt adds.

Staying with GDPR, it says data regulators across Europe may soon bear their teeth and impose monetary penalties for a full range of breaches under the relatively new regulation, not just those associated with security.

Meanwhile, a significant development in Ireland is raising awareness of multiparty actions due to breaches of data protection rights. A civil liberties group plans to submit a legal complaint on behalf of over 1,000 people, which may set the stage for proposals contained with the Representative Action Directive.

"The Irish Government introduced a Public Services Card which the Data Protection Commissioner considered was in breach of the GDPR," Allnutt explains. "The DPC concluded that the manner of information collection and retention on millions of citizens was unlawful and is planning to launch enforcement against the relevant government department."

A shift in approach

Embracing technological change and all the opportunities it presents means identifying and embracing the threats and accelerating and incentivising solutions through an ongoing commitment to investment and cooperation.

To this end, the World Economic Forum is working on a project focused on increasing global cooperation between the public and private sectors in addressing key challenges to security and trust in the digital landscape. The aim of its *Future Series* project is to understand how the key technology waves of the near term will impact the threat and risk landscape in the future, how these technologies will change the cyber security landscape and the subsequent security and response implications for countering these developments.

That cyber as a top risk issue is widely acknowledged, and never refuted, but the risk persists as technologies evolve, and as new doors are opened up – both in terms of new and exciting developments and in terms of the vulnerabilities, as cyber criminals seek new ways to exploit each new door opened.

And while the last few years have seen dramatic technological change, it's nothing compared with what's in store.

Cyber readiness, key to survival

So much is said and written about cyber risks and how to prepare for them, but, as ever, the devil is in the detail. In this in-depth analysis, Xavier Marguinaud offers a framework for companies looking to achieve comprehensive 'cyber readiness'

Lately, we are hearing more and more new cyber-related terms such as cyber index, cyber institute, cyber program, cyber review, and cyber readiness, to name a few. The latter is one that is trending right now. Unfortunately, as this is a relatively new term, most explanations surrounding the concept often only provide a high-level overview without going into detail. So, what is cyber readiness exactly?

If 'readiness' is the state of being fully prepared for something, we could easily define 'cyber readiness' as having everything programmed and in place to minimise any possible effects stemming from a potential cyber incident. If that is so, then we understand that the goals of cyber readiness are to detect, contain and mitigate these consequences. Therefore, cyber readiness would imply that any potential impacts of a cyber incident are envisaged and will be limited so that a company can return to business quickly.

There are several ways of describing the cyber readiness framework and all its components. For the purposes of this article we will reference the one provided by the Cyber security & Infrastructure Security Agency. In 2019, this US governmental entity linked to the department of Homeland Security released a set of recommendations about cyber readiness to help companies implement organisational cyber security practices. This approach, in particular, stands out for being original in its communication yet consistent with the NIST Cybersecurity Framework and other cyber security standards.

CISA's approach

There are six essential elements in CISA's approach:

1. **Yourself – the leaders** emphasises governance and the importance of having board members and top executive management involved in designing, investing and driving the company's cyber security strategy. Cyber security should be handled as a business risk and companies should understand that it takes time and money to define and implement a relevant strategy.

2. **Your staff – the users** focusses on encouraging the development of a cyber security culture among employees and external stakeholders (service providers, customers, etc.), improving everyone's vigilance. Awareness of your staff, which can only be achieved through training and education, is key. Remember that they might become your first line of defence!

3. **Your systems – what makes you operational** highlights that protecting critical systems is one of the most important actions to take in cyber security. It is crucial to know what your critical systems are and where your most valuable information resides. Companies should build security into and around these assets. Therefore, drawing up a risk map and performing a data/system classification are two unavoidable exercises.

> **"Cyber readiness would imply that any potential impacts of a cyber incident are envisaged and will be limited so that a company can return to business quickly"**

4. **Your surroundings – the digital workplace** recommends companies ensure that only those who belong to their digital workplace have access to it. Granting appropriate access and setting up relevant rights should be a priority. Any digital environment needs limits.

5. **Your data – what the business is built on** sets out to convey that making back-ups and avoiding loss of information is essential to the company's operations. It may seem obvious to most of us, but I think it is worth repeating over and over again. The CISA guide recommends establishing regular data backups and redundancies for key systems along with protecting backups using encryption and offline copies.

6. Finally, one of the main goals in cyber security for any company should be to limit damage and speed up the time it takes to resume normal operations. The final step, **Your actions under stress – what to do?**

puts the onus on companies to make their reaction to cyber attacks and systems failures an extension of their other business contingency plans. It is highly advisable to plan and prepare drills for cyber attacks as you would for fire drills or any other tangible threats.

The CISA document itself also encompasses some guidance for IT professionals. It is a single and common document that gathers information for both leaders and IT teams working for the same company. This is a brilliant idea!

Although all six of CISA's steps are relevant and imperative for a company's survival in the face of one or more cyber threats, the sixth is of particular importance. The business continuity plan can only be prepared if all other steps have been completed. To complete the BCP, several stakeholders within the company, who may not normally interact with each other, need to come together on an ultimate common goal: survival.

If the BCP has been correctly prepared, then the company can bounce back. The incident response plan, which forms part of the BCP, plays an essential role in ensuring cyber readiness.

The incident response plan structure

A relevant incident response plan is usually made of three key elements: plan, team and tools.

Firstly, the plan addresses the question: what are we going to do to deal with the threats? Here, we must consider concepts such as containment, eradication, and escalation.

Secondly, the (centralised) team addresses the questions: what kind of expertise do we need? what would the team members' responsibilities and authorities be? Ideally, any incident response team should be made of the following seven people: response manager, security analyst, lead investigator, threat researcher, communication leader, documentation leader, HR/legal representative.

Thirdly, having the (adequate) tools addresses the question: how will we be handling the incident? The company needs a set of analytical, alerting and remediation tools: cold/warm/hot sites, SIEM, IDS/IPS, NetFlow analysers, and so on.

When addressing all three elements in the Incident Response Plan, one must keep in mind the three ultimate goals of any incident response strategy: analyse, report, respond.

So, this explains how the plan is structured and why. However, from my point of view, as a cyber insurance underwriter, a comprehensive cyber incident response plan needs to be elaborated.

The incident response plan – Contents

From experience, we like to see the following six elements in the incident response plan:

Preparation: Define policies, conduct risk assessment, develop communication plan, outline roles/responsibilities/procedures/authorities, recruit and train team members, set up appropriate tools.

Identification: Decide what criteria calls the team to action, identify and assess the incident, gather evidence, establish the severity scale, use the escalation protocol.

Containment: Isolate the security incident (the aim is to stop further damage), short-term containment, systems backups (take a forensic picture before wiping affected systems!), long-term containment.

Eradication: Isolate the root cause of the attack, identify and mitigate vulnerabilities to stop further attacks (this might change the configuration of the organisation, so the aim is to minimise the effect on operations).

Recovery: Bring affected (and therefore decontaminated) systems back into their production/working environment.

Lessons learned: Improve both the production/work environment and the Incident Response Plan.

A cyber essential

So, to recap, I hope to have given sufficient detail to provide a good understanding as well as some much-needed depth to the concept of cyber readiness – this term that we seem to hear all too often nowadays without knowing what it really means in practice. I also hope to have emphasised just how essential cyber readiness is as part of any company's strategy, and which can help unite company stakeholders in preparation and readiness to confront the inevitability and reality of cyber threats today and tomorrow.

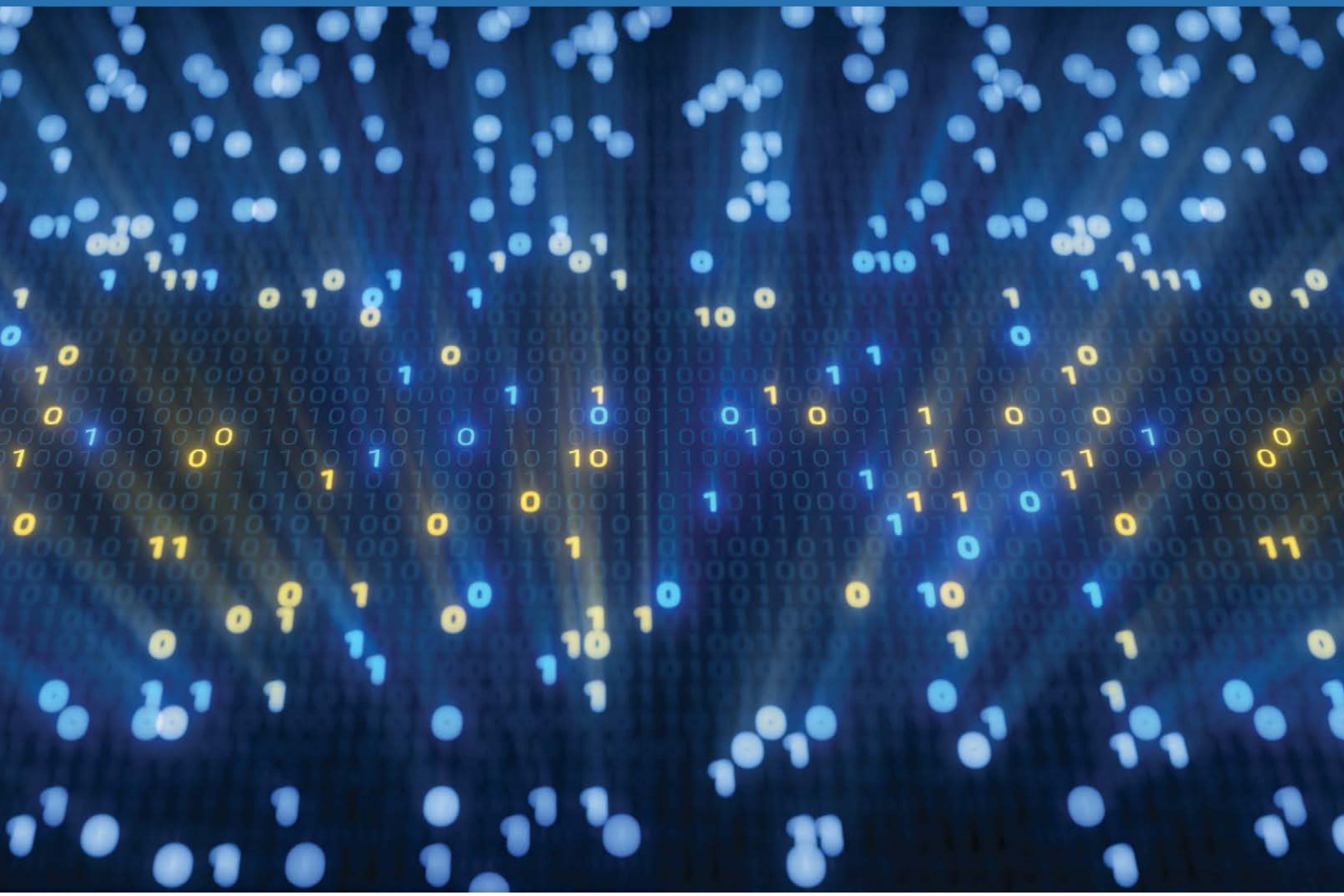
In essence, companies should be asking themselves just how cyber-ready they actually are. When they seek appropriate insurance, this is one of the first questions that will be on the table.

Xavier Marguinaud, Cyber Underwriting Manager
Tokio Marine HCC
xmarguinaud@tmhcc.com

Tel: +34 93 530 7439


Different
by design
The only SaaS platform to provide integrated solutions to the entire insurance value chain: Risk Managers, Brokers, TPAs, and Insurers
ORIGAMI RISK
info.origamirisk.com/CIR-2020

CIR
CONTINUITY INSURANCE & RISK



Lighting the road ahead. David Adams considers how end user requirements are influencing the development of more complex, integrated solutions, fit for an age of interconnected organisations. Page 32

A solution to data silos. Risk management software is now an important, strategic tool. Today, it can even be the answer to one of the greatest organisational headaches: breaking down silos. Neil Scotcher explains how. Page 34

RISK SOFTWARE REPORT 2020

Lighting the road ahead

David Adams considers how end user requirements are influencing the development of more complex, integrated solutions, fit for an age of interconnected organisations

In recent years risk management has been transformed into a vital business function, supporting and informing strategic decision-making. That has led to the need for risk management software to become more dynamic, more sophisticated and more flexible, to fulfil the requirements of an increasingly diverse group of end users.

Earne Bentley, president, risk solutions, at Origami Risk, suggests that one of the most significant changes in recent years has been an increased focus on a wider range of operational risks. His view is in line with the findings of recent research from the Institute of Risk Management, which found that 81 per cent of more than 100 risk professionals it surveyed said they use risk software to focus on operational risk.

But the technology is used for many other purposes too, from internal audit to management of business continuity, compliance and legal risks. As its scope has grown, so too has risk management; in effect, it has become everyone's business.

Changes in how the software is used are also due in part to a decisive move towards use of cloud-based solutions during the past decade. Using cloud and software-as-a-service (SaaS) approaches has cut the cost of sophisticated solutions, bringing them within the financial range of more organisations; and it means the software can be deployed in different ways, with risk information now being fed into the system from across the organisation.

In effect, enterprise risk management software has become, as Anton Lissone, chief technology officer at provider, SAI Global, puts it, both an enabler of continuous risk assessment; and "a decision-making system, rather than a system of record".

Artificial intelligence

Whatever the purpose for which it is used, at the heart of an effective risk management solution is the ability to gather and analyse very large quantities of risk data, drawn from inside and outside of the organisation. The software needs to be able to filter this information, to feed relevant information to the individuals, teams and business systems that need it.

Use of AI and natural language technology is slowly replacing use of preset business rules as the basis for these processes. For example, natural language processing in SAI Global's risk software is now used by financial services companies to parse regulatory updates issued by the Bank of England, identifying which of the company's controls or processes need to be adjusted.

Risk data collected inside an organisation must be supplied by individual risk owners, many of whom are not risk specialists themselves.

"Risk technology is used for many purposes – from internal audit to management of business continuity, compliance and legal risks. And as its scope has grown, so too has risk management; in effect, it has become everyone's business"

Vendors have dedicated more time to improving the user experience and design; and the visual presentation of risks, to make the systems easier to use. For example, Ventiv's risk management solutions may be integrated with Ventiv Digital, a survey-style front end accessible to ordinary users via mobile devices or desktop PCs.

Bentley says many Origami end users now expect to buy an integrated risk platform that can be used across different departments, linked using APIs to enable real time transfer of risk data between business systems. Other end users take a different approach: they may start using the software for a single purpose, then extend its scope later.

For example, logistics company DHL originally implemented Origami to manage claims, but has gone on to commission a fully integrated risk solution. The company self-insures, using the software to manage risks in the UK and Ireland, countries in eastern Europe, the Middle East and Africa. Staff can use the mobile Origami app to report risks, incidents or accidents, triggering investigations and corrective actions. If a DHL driver is involved in a road accident, for instance, the driver can call a contact centre managed by a third-party service provider, from where an automated alert is sent to the Origami software. This then creates an accident investigation, alerting the manager for the relevant geographical area and delivering information about the accident.

DHL is now creating a specific area within their implementation of Origami for each of its 700 site managers, who will be able to log in to review accident investigations that are still outstanding; and the live status of accidents and claims relating to their site. In addition, any clients seeking to make a claim in relation to (for example) a late delivery, or damaged goods will also soon use Origami to start this process. This aspect of the system became available to DHL customers in the Czech Republic from January and will be rolled out across the rest of the region during 2020.

"It's bringing together lots of data that was previously generally stored offline, in spreadsheets or different standalone systems, tying all these siloes of data together into one platform," says Julian Thomas, head of processes and systems at DHL. "The visibility that provides, having that data at my fingertips, is light years ahead of where we were before. It's automating manual processes and removing duplicate processes. We've got one version of the truth now that all of us can look at."

Ventiv managing director Steve Cloutman also highlights another common demand from larger end users: the ability to exchange data more easily with third party organisations. One example of this can be seen in work the company has completed with Zurich and one of the insurer's most important clients, Nestle. The two companies' systems are now effectively linked, via Ventiv's technology and APIs, giving Nestle immediate access to claims, policy and risk data.

"DHL is now creating a specific area within their Origami implementation for each of its 700 site managers, who will be able to log in to review accident investigations that are still outstanding; and the live status of accidents and claims relating to their site"

Of course, working more closely with other organisations will also generate new risks. Mark Holt, managing director, EMEA and APAC, at Riskonnect, suggests that cyber, compliance and reputational risks will all become a bigger concern for more organisations as "business models become increasingly intertwined with third parties, whether that be a supplier, customer or partner". He says a growing number of Riskonnect end users are implementing its Third-Party Risk Management solution, which automates third party onboarding and compliance management processes through digital portal technology.

Other organisations are motivated by a desire to face down risks that affect their people. Rich Cooper, director of global accounts at Fusion Risk Management, says some of its end users are now focusing on physical threats to people or assets. He cites the example of Fusion clients in Hong Kong that were forced to lock down or close business premises during political protests. "They're building their risk frameworks around where their people are."

The tendency to use risk software for these many different purposes is also encouraging more integration of the software with other business systems. In some cases the software may become part of an integrated GRC function. David Bergmark, CEO of another vendor, Protecht, says integration has become a key element in service delivery for many of the company's larger clients, in multiple sectors: its software may be linked to clients' ERP platforms, enabling those business systems to access customer or product data related to incidents, investigations and complaints being processed by Protecht's ERM solution.

"The tendency to use risk software for these many different purposes is also encouraging more integration of the software with other business systems. In some cases the software may become part of an integrated GRC function"

Software development and the demand for these and complementary products is also driven by regulatory requirements. Holt says regulatory changes are boosting demand for Riskonnect's ERM, compliance and third-party risks management solutions; and for subscriptions to its Unified Compliance Framework, which provides access to more than a thousand different regulations via APIs.

But above all, the shift towards use of integrated risk solutions comes from the strategic value such solutions can offer, as organisations of all kinds seek to prosper in an ever more digitised environment. "Having the right risk management tools in place needs to be a strategic priority, to enable digital transformation, not a nice to have," says Holt.

Bentley also believes the transformation of risk management into a truly strategic function will encourage integration with other business systems. "You're going to see a wider adoption of the concept of risk being seen as strategic through the organisation," he says. Using risk software will help an organisation to understand where it is going, while ensuring it progresses towards its goals as safely and securely as possible. It has become more difficult to sum up quickly everything that the software can do – but also very difficult to go on without it.

A solution to data silos

Risk management software is now an important, strategic tool. Today, it can even be the answer to one of the greatest organisational headaches: breaking down silos. Neil Scotcher explains how

Across the insurance value chain, those working to improve collaboration, reduce costs, and capitalise on new opportunities often find themselves fighting an uphill battle, their efforts hampered by the limitations of technologies used for the collection, management, and analysis of critical risk and insurance information.

At the heart of the problem is a disconnect between these technologies – whether spreadsheets or disparate software systems in place within organisations. A lack of integration may lead to a reliance on manual processes that, in turn, increase the likelihood of error. The inability of multiple systems to 'talk to each other' can also mean that there is no single source of truth when discrepancies arise. And given the negative impact on the ability of insurers, brokers, and risk managers to take the larger picture into account as they strive to take a more strategic approach to underwriting, assessing, and mitigating risk, perhaps most problematic is the siloing of data.

Edd Wilder-James, in the Harvard Business Review article *Breaking Down Data Silos*, describes these silos as isolated islands of data that complicate and make more costly any advanced data analysis initiatives. According to Wilder-James, while numerous factors give rise to data silos, it is ultimately access to data that is the greatest obstacle to analysis.

"Those evaluating risk have three questions," explains Said Taiym, chief digital officer at Lockton Companies. "In terms of rates, exposures, policies, and coverage, how is my organisation doing compared to last year? How are we doing in comparison to others in my industry? And how are we doing in relation to businesses of similar size? Without the right information, these questions cannot be accurately answered."

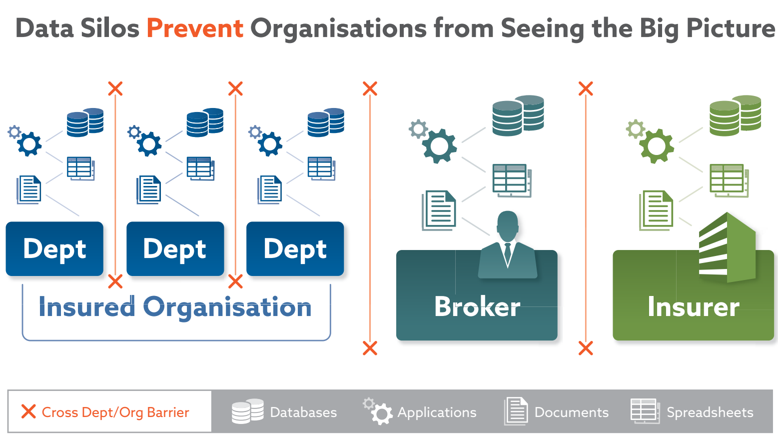
How Origami Risk helps break down data silos

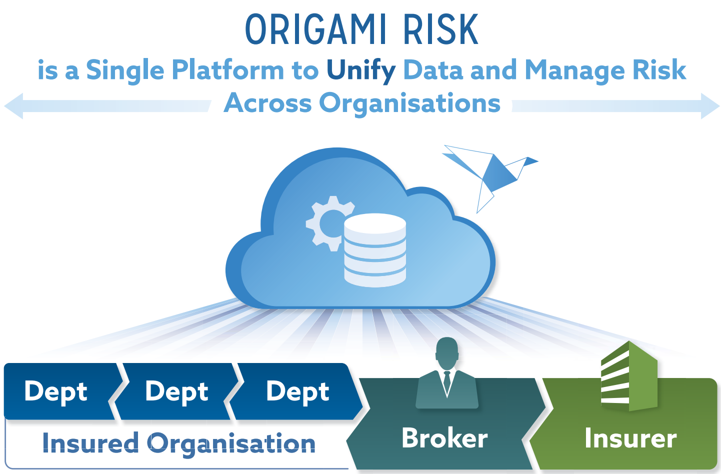
For risk managers and brokers, the annual process of collecting and analysing the exposure values used for policy renewals is often impacted by data silos that require a great deal of effort to overcome. The process requires sending multiple, 'one-off' emails to request exposure values and follow up on status. Data collected from various users' locations/clients must then be aggregated, which usually requires that data be copied and pasted from individual spreadsheets into a master document or system. Each additional step introduces the potential for errors or omissions which can contribute to an organisation overpaying for premiums or being underinsured.

With features such as automated collection workflows, data collection portals, and dashboards for status monitoring and tracking, the Origami Risk platform is a technology solution that aims to simplify data collection for insured organisations. Exposure values data is brought together in a single system with location, insurance, and claims information. This provides risk managers and brokers with the ability to take full advantage of the data, using reporting and analysis make informed decisions that contribute to more accurate premium pricing and help ensure that properties are insured-to-value.

The Origami Risk platform also provides a centralised tool for insurers to collect exposure data across various insured organisations needed to process renewals and eliminates the need for maintaining multiple spreadsheets.

In addition to improving the exposures collection in the renewal process, online portals and customisable dashboards can





also improve the way information is shared with brokers and insured. Via online portals, agents and insured policyholders can easily lookup and view the policy and claim information for which they have access rights, view a history of premium contributions, update information needed for renewal, and check the status of endorsements.

"Origami enables us to consolidate all of our risk management-related information in a single database and to distribute and share discrete data for each of our operations with our senior leadership," says Jeroen Helders, group treasurer and insurance risk manager at Royal Cosun. "We can also deliver timely and accurate underwriting submissions to all of our insurance company providers. With ready access to this data, our property insurers are able to underwrite our risk with greater precision, which has translated to reduced premium costs."

Aligning strategy and driving meaningful change

Even with improvements in the collection of data and the tools available for calculating renewals, the introduction of a technology solution is not a panacea to the challenge of siloed data. Removing those barriers requires a well thought out approach that is aligned with the strategic goals of the organisation and is fully integrated across the enterprise. Without it, organisations run the risk of recreating what Wilder-James refers to as "a whole new set of silos, albeit with advanced capabilities."

Unfortunately, such outcomes were not uncommon over the past decade as organisations rushed their governance, risk, and compliance efforts in response to the 2007–2008 financial crisis. For example, where one group focused exclusively on matters related to regulatory compliance, another was putting into place controls designed to assess and mitigate reputational risk; yet another was tasked with monitoring the status of internal compliance initiatives. All too often, there was no overarching view of how all of these efforts tied together in support of a broader strategy, or how gaps or failures in one area impacted the entire enterprise.

Just as GRC programmes must be unified in support of defined strategy rather than fragmented or isolated in departmental or functional silos, the technology used to support GRC programmes should contribute to the elimination of data silos. Success depends upon it.

The flexibility of the Origami Risk GRC solution makes it possible to customise the system to meet the unique needs of an enterprise and its stakeholders. For example, formulas for calculating and rolling up risk (sub factors) can be customised so that this data-driven process actually matches the tolerance and appetite of the organisation. The solution also allows for data to be exchanged across departments and functions through the sharing of common objects such as risk libraries and controls. Features such as lenses contribute to the ability of different groups to look at the same data in entirely different ways.

Benefiting from a single platform solution

The full integration of risk and insurance technology helps to eliminate data silos by equipping organisations with the ability to see the big picture while also ensuring a unified view of the multiple processes and specific points of data that matter most to individual stakeholders. Within a single cloud-based platform, Origami Risk offers a full suite of risk management and insurance core system software. Highly configurable and completely scalable, these tools deliver efficiency and convenience, serve as a single source of truth, and provide users with access to the risk and insurance data necessary for making informed decisions, reducing risk, and achieving desired outcomes.

To learn how the Origami Risk platform can play a part in eliminating data silos and contribute to your success, visit info.origamirisk.com/CIR-2020 today to download a case study, sign up for our newsletter, or request a demo.

ORIGAMI RISK
ORIGAMI

Origami Risk is a leading provider of a unified SaaS solution for the risk and insurance industry—from insured corporate and public entities to brokers and risk consultants, insurers, TPAs, and risk pools. Origami's solution is differentiated by:

- Best-in-class service model
- Highest NPS Score for RMIS providers
- Highly configurable, without the need for custom development or plug-ins
- Secure, cloud-based software accessible via web browser and mobile app
- Easy to use and automated data and analytics tools, including portals, dashboards, and reporting, with varying levels of access for internal and external users
- Software designed and supported by industry veterans with a balance of risk, insurance, and technology expertise

Origami Risk provides risk managers, underwriters, finance/accounting professionals, and claims administrators with the tools to break down silos that exist within or between organisations. From a single platform, organisations are able to aggregate data from multiple sources, more easily analyse and report on it, and use it to automate processes – generating time and cost savings. Solutions available in Origami include:

- Policy, Claims, & Incident Administration
- Exposure Values Renewal Management
- Total Cost of Risk (TCOR)
- Captive Management
- Integrated Governance, Risk & Compliance (GRC)
- Health & Safety Management
- Asset & Fleet Management
- Certificate Tracking
- Audit / Survey Management Tools (Online / Offline)
- Underwriting

Ongoing deployments and seamless system integrations

The Origami platform is a true SaaS, multi-tenant system. Highlights include:

- A Single Version of the application is maintained, meaning all clients are on the same version. No client falls a version or two behind and there is no sun-setting of support on versions.
- Releases Deployed Quarterly to quickly respond to clients' ever-changing needs. This ensures greater stability by avoiding large, complicated upgrades. It also ensures clients derive ongoing value from critical features, rather than waiting for new features to be deployed months later. Upgrades are provided at no additional cost.
- Seamless Integration with third-party applications without the need for custom development.
- Data Integration Tools managed by on-screen automated file import/export tools to facilitate system integrations of varied complexity and frequency.

Experienced service team aligned with client objectives

Origami partners with its clients by providing:

- Dedicated Collaborative Service Team to answer questions or respond to issues.
- Award-Winning Implementations with a configurable system and a service team that possess a balance of industry and technological knowledge.
- Continuous Expert Access as the implementation team also provides ongoing support post-implementation. This means support teams know each client and their business, how they use the system today, and their plans for tomorrow. It also eliminates the knowledge loss experienced during the handoff from implementation to support.

A singular focus on helping clients achieve their business objectives underlies Origami's approach to the development, implementation, and support of risk management and insurance core system solutions.

To learn more about Origami's solutions and to request a demo, go to info.origamirisk.com/CIR-2020

BARNOWL GRC & AUDIT
BARNOWL

BarnOwl is a fully integrated risk management, compliance and audit software solution implemented in over 200 organisations. The software aims to support best practice in risk management, compliance and audit frameworks including COSO, ISO 31000, the Generally Accepted Compliance Practice Framework and International Professional Practice Framework, in a parameter-driven environment.

BarnOwl supports effective strategic and operational planning, simplifies and facilitates regulatory compliance, drives combined assurance and integrated reporting and embeds accountability and ownership for the management of risk, compliance and assurance.

BarnOwl Risk facilitates a structured and systematic approach to risk management by providing a way of prioritising and managing risk and opportunity across the organisation in pursuit of business and strategic objectives. It supports a unified view of risk and gives management and staff at every level the ability to identify, assess, manage, monitor and report on risks.

BarnOwl Compliance facilitates compliance through the automatic generation of compliance risk management plans and checklists. Online checklists and action plans are sent out automatically to the relevant compliance owners, supporting compliance monitoring and remedial action.

BarnOwl Audit facilitates the full internal audit lifecycle, including planning, execution, reporting, monitoring and follow-up, helping user organisations streamline and standardise internal audit processes.

The audit module is fully integrated with the risk module, supporting true risk and control-based auditing. The product's final audit reports (integrated with MS Word) and business intelligence dashboards help organisations to gain insight into audit findings, root cause analysis, risk analysis, trends and benchmarking.

BarnOwl Business Intelligence provides interactive, drill-down dashboards transforming risk, compliance and audit data into valuable business insight and foresight. The Power BI dashboard can be used to visualise and analyse risks, controls, KRIs, incidents, action plans, compliance checklists, audit findings, audit projects and timesheets.

barnowl.co.za

CORPROFIT
CORPROFIT SYSTEMS

KnowRisk is packaged software that is generally configured using tools provided in the application, supplemented by customisation that users specify as and when required. The software implements a three-tier architecture with a Windows thick client front-end which is installed on a user's machine or a thin-client platform using Citrix or the cloud.

Central to KnowRisk are rich knowledge bases, allowing different organisations to share knowledge and improved risk and governance processes yet still allowing each organisation to hold onto its own ways of doing things.

The KnowRisk database, which is implemented in MS SQL Server or Oracle, is the heart of the entire architecture and all other components and sub-components integrate with it via the application server or the DataMart.

KnowRisk Forms are an extension of the KnowRisk UI and consist of standalone forms that may or may not be linked together. The forms are particularly suited to users that do not have the need for the advanced features of the KnowRisk Classic interface. Forms provide functionality for business rules to be embedded, data entry, data views and steps in an overall workflow. KnowRisk has built-in reporting capabilities based on Crystal Reports and surfaced via the KnowRisk Classic UI. This is bundled with the software so there are no extra licensing costs associated with it.

This product also allows users to export a subset of the database into a DataMart that can be easily used by a business intelligence tool to provide advanced data modelling and visualisations. This popular feature gives users the flexibility to plug in their own BI tool to obtain customised reporting and dashboards out of the risk management system. KnowRisk is a fully quantifiable system and performs a range of calculations whether patently exposed or not.

All calculations in KnowRisk can be viewed subjectively (using words) and quantitatively (using figures) and the database automatically synchronises between the subjective and quantitative values – helping users to understand the true meaning of the numbers.

corprofit.com

CORUSON
IDEAGEN

Coruson is enterprise cloud-based safety software designed to provide organisations with complete control, visibility and real-time reporting of every detail and aspect of safety and operational risk. The software manages safety, incident reporting and risk to help support users with compliance. It employs a risk-based model to modernise business processes. Coruson is designed to support integrated risk management via centralised risk registers; definition, modelling and documentation of risks; risk visualisation and communications via BowTie methodology and dashboards, mitigation, action planning and automation; incident reporting via smart forms and geo-tagging; and quantification and analysis.

ideagen.com

ENTERPRISE RISK MANAGER
RISKHIVE

This product can be configured to meet a range of requirements and reconfigured as many times as necessary, to suit the user organisation's own development and increasing levels of risk management maturity. The system offers fast deployment times, with a secure cloud system commonly operational within 24 hours. During configuration, using the import wizard, existing risk registers can be migrated into the system from Excel or direct data transfer. They can then be consolidated and aggregated, giving instant data roll-up, storage and maintenance across the portfolio within a user-defined hierarchy. RiskHive supports the import of current Excel risk registers, replicating their familiar layout and data fields on the main user interface. This also reduces the need for training. Users access the system via an intuitive, browser-based interface which allows real-time search and saveable filter functions on database fields.

Graphical and interactive BowTie functionality is provided to help describe cause, risk and effects, alongside any controls, responses and fallback positions. An inbuilt word cloud generator with duplicate/repeated word and sentence analyser helps streamline and visualise categories and commonalities of risk. For geographical representation of risks, there's an interactive world map view of projects or risk concentrations, with navigate-to feature. The risk radar Gantt view of risks on a timeline includes milestones and budgetary allocation dates. An interactive risk waterfall generator combines multiple scenarios, metrics and timescales, backed up by a selection of detailed database field completion reports and exports.

For management reporting and oversight there are multiple graphical dashboards covering portfolio, programme, project and risk-level reports. RiskHive allows cost and schedule risk analysis – separate or combined – along with Monte Carlo simulation for companies that wish to quantify their risk profile and/or run a cost benefit analysis on the efficacy of controls and mitigations. This system can be aligned to ISO / COSO standards and supports multiple languages and currencies, which may also be used simultaneously.

riskhive.com

FUSION FRAMEWORK SYSTEM
FUSION RISK MANAGEMENT

FUSION RISK MANAGEMENT

The Fusion Framework System eliminates the need for separate modules across the many areas of risk and business continuity management. Users are encouraged to share ideas, best practices and solutions to address common challenges.

Fusion Connectors, including Everbridge, Onsolve, xMatters, ServiceNow and NC4, enjoy integrated workflows, feature access and data sync. Practitioners that use Fusion Connectors are able to manage multiple workstreams of activities during an incident or exercise and gain control over any event through the one system.

Fuel, Fusion's advisory consulting services, provides a range of resources enabling programme leaders to focus on higher objectives, mature their programmes faster and more effectively. End user companies include Box, Cambia, TBK Bank, TransUnion and AQR.

fusionrm.com

GOAT RISK
GOAT RISK SOLUTIONS

GOAT Risk is a cloud-based solution that aims to bring data into the risk dialogue. It is designed to presents a single point of access for all key data in the business, creating a 'corporate memory' of all risk incidents.

The tool includes risk management tips and tricks and user FAQs to raise the risk awareness across the user organisation.

goatrisksolutions.com

HOPEX IRM
MEGA INTERNATIONAL

HOPEX Integrated Risk Management solutions aim to help users efficiently identify risks and implement related controls in a structured library.

With this product, risk and control assessments can be performed through automated assessment campaigns. The solution also enables users to declare incidents and contextualise them. Users can also manage compliance, and map regulatory requirements to processes and IT assets.

Assessment templates are provided so users can quickly assess risks and controls; and integrated information on risks, controls, incidents and regulatory requirements are available in a consolidated view. A personalised to-do section allows users to manage daily activities in an efficient manner, and multiple widgets enable users to build custom dashboards and monitor key indicators. Action plans and collaborative workflows are available out-of-the-box to efficiently mitigate risks.
The Internal Audit module offers a variety of reports and recommendations on the status of risks, compliance and processes, as well as risk and performance analysis. Key functions of this module include planning and control, access rights, audit staff management and approval workflows for preparation, implementation and follow-up.

This solution provides a variety of functions, templates and automatically generated documents that standardise, automate and make processes reusable. It provides a single, real-time, auditable repository to consolidate information in a consistent manner and ensure the reliable follow-up of recommendations that are linked to findings and action plans.

The Audit Offline feature allows auditors to run audits in remote locations. Auditors can implement and deploy audit plans through mobile application and upload documents of their findings and recommendations.

Mega releases three updates of this product per year, with 3.1 the latest available. This solution will integrate with any third-party vendor through open APIs.

mega.com

JCAD CORE
JC APPLICATIONS DEVELOPMENT

The JCAD CORE RISK application has been designed to offer organisations struggling with in-house tools an alternative that is simple to use and implement but that also offers a breadth of risk and compliance functionality.

Through configuration, a team of consultants will set up the application to mirror those aspects of risk and compliance management that are unique to each organisation, for example reporting structure and terminology. Going forward, full training is provided so that users can be totally self-sufficient in the administration of the application and not reliant upon JCAD, though support is available when required.

Essentially, JCAD CORE is designed to help users identify, monitor and mitigate risk; embed risk management throughout the organisation; ensure corporate compliance; capitalise on new opportunities; drive effective business strategy and improve efficiency. Features include interactive dashboards, multiple registers, performance metrics and automated alerts. This web-based solution is suitable for both small and large organisations looking to improve upon how threats and compliance are managed. On G Cloud.

jcad.co.uk

JCAD LACHS
JC APPLICATIONS DEVELOPMENT

JCAD provide easy-to-implement software for streamlining risk management and claims handling processes in the public and private sectors. JCAD LACHS claims management software was first developed 25 years ago to enable organisations to improve upon the efficiency and productivity of their claims team. Retaining this function in-house ensures access to valuable historic data regardless of insurer and can help drive down claims and premiums.

JCAD have vast experience in this field ensuring data is clean, validated and fit for purpose – and can also apply GDPR retention policies. Its latest incarnation is LACHS Version 5, which has an abundance of new features including interactive dashboards, geo-mapping and document bundling. Additional modules, such as integration with the MOJ Portal and online claim form submission are also available, making the JCAD software the central point of the claims team. It is designed to provide a high level of functionality to busy claims processing departments, improving customer service and reducing operational costs. As an off the shelf solution, it is also quick to implement and cost effective to maintain.

jcad.co.uk

MACLEAR
MACLEAR

Maclear helps small, medium and large organisations across the globe achieve their integrated risk management goals, including governance, risk and compliance.

The Maclear eGRC Suite is a comprehensive, proprietary solution for capturing, monitoring, measuring and managing integrated risk and compliance across the enterprise. The functional capabilities of the solution help strengthen corporate governance processes, facilitate effective risk and compliance management and convert data elements into actionable data.

This product is designed as a modular, scalable tool that enables continuous monitoring and provides transparency into enterprise-wide risk posture. A suite of applications built on a highly configurable and extensible software platform provides the necessary foundation to break down the enterprise silos by leveraging a common GRC data repository, framework and language, while supporting incremental adoption.

Maclear eGRC Suite enables businesses to quickly address immediate pain points, mitigate risks and successfully manage the complexity of the dynamic modern regulatory and compliance environment. The Maclear software solution enables effective monitoring in the form of dashboards, macro-level analysis and automated workflows for reporting, assessments and remediation management. The solution also provides for operational support through configurable controls, access automation, testing and integration with third party tools.

Designed as a modular suite of products that integrate seamlessly to provide a complete and dynamic solution; modules can either be implemented individually or collectively – as needed.

maclear-grc.com

PENTANA RISK PRODUCT MANAGER
IDEAGEN

Pentana Risk is a cloud-based enterprise risk management software solution that integrates risk management processes, from identifying and assessing risk across the business and assigning and monitoring mitigation plans, through to reporting and defining long-term strategy.

This product was designed to help users establish a framework that allows them to manage operational, financial, IT and strategic risks in a single risk management system. The software provides real-time metrics on all aspects of risk, such as performance, processes and assets.

ideagen.com

PREDICT!
RISK DECISIONS

The Predict! solution aims to provide users with a complete integrated risk capability Predict! Risk Controller manages, assesses and reports on opportunities, threats and issues, Predict! Risk Analyser is used for Monte Carlo cost, schedule and business scenario analysis, while Predict! Risk Reporter is dedicated to custom reporting

With Predict! Risk Analyser, message-driven prompts encourage users to engage in managing risks and actions. With combinations of risks and visuals, lists offer ad-hoc risk reporting, across the entire business or at any drill-down level. Monte Carlo risk analysis provides up-to-date contingency information for strategically important risk-based decision-making.

Predict! Risk Analyser is a single tool for project and programme analysis and bespoke uncertainty modelling to support executive-level decision-making. It helps users test the resilience of a schedule and budget, pinpoint key risk areas affecting completion and demonstrate the benefit of mitigation actions.

Automatic summary reports enable users to communicate outcomes confidence quickly, while the interactive dashboards drive understanding and facilitate discussion.

riskdecisions.com

PROTECHT.ERM
THE PROTECHT GROUP

This tool aims to help users dynamically manage all risks in a single platform, including risks, compliance, health and safety, internal audit, incidents and key risk indicators; and automates the manual and time-consuming processes of managing the collection and analysis of risk information across the organisation.

Key functionalities include a complete GRC and risk management platform, mobile app, dynamic form builder, workflow management, bulk update, integration with other systems, BI and risk analytics dashboards and reporting and optional regulatory content.

The implementation of Protecht.ERM is completely scalable, assisted by easily deployable best-practice templates for risk assessment, incident reporting and auditing. Alternatively, users can create their own data capture forms, workflows, dashboards and reports – with no IT or coding skills required.

This tool was designed by risk managers for all kinds of user and is configurable to specific business processes. Scalable and accessible anywhere, Protecht.ERM is also designed to work for any organisation, regardless of size, industry or risk maturity stage.

protechtgroup.com

Q-PULSE
IDEAGEN

Q-Pulse is an on-premise or hosted application designed to help organisations identify emerging risks and opportunities, comply with regulations and standards and streamline the management and reporting of quality and safety. The system aims to help users to connect all processes of a QMS in one system. Q-Pulse enables users to enhance the effectiveness of their organisational knowledge base, providing access to complete up-to-date information to enable the identification of improvement opportunities. For risk management specifically, Q-Pulse helps to maintain a central risk register, providing effective management oversight of risk.

ideagen.com

QUANTATE RISK
QUANTATE

Quantate provides a range of web application software to support risk and compliance activities, delivered as Software as a Service. Dashboards show personal information such as key responsibilities, tasks to perform, their reports and issues raised or escalated for their attention as well as jump-off points to the relevant parts of each application.

Quantate Risk is an enterprise-wide risk management application that provides a platform to support the management of risk frameworks to cater for the diverse risk contexts that exist throughout an organisation. Highly configurable, it is designed to allow frameworks to be built in a hierarchical manner.

Quantate Compliance provides a platform for the management of obligations which may be legislative, procedural or contractual. Frameworks can be configured by the user to be simple or sophisticated, depending on the requirement. Quantate Project is a risk management application that is focussed on managing the risk within projects. Cost exposure can be aggregated at a cost level and over time to show risk exposure within portfolios and programmes. Critical path exposure allows for schedule impact to be quantified. Quantate Project uses industry standard statistical techniques such as Monte Carlo to produce risk exposure profiles.

Quantate application reporting is carried out through a configurable reporting engine where reports can be generated and saved for future reference and accessed via user dashboards. Quantate products are designed to work on all devices, both desktop and mobile. These tools are used in infrastructure, local and central government, education, healthcare, retail and construction.

quantate.com

RISKONNECT
RISKONNECT

Riskonnect is designed to empower organisations to anticipate, manage and respond in real-time to strategic and operational risks across the extended enterprise. More than 900 customers across six continents use this tool to gain previously unattainable insights that deliver better business outcomes. This provider has more than 500 risk management experts in the Americas, Europe and Asia.

riskonnect.com

SAI360
SAI GLOBAL

SAI360 offers solutions to help with compliance management, operational risk, IT and digital risk, data privacy, internal controls, internal audits, business continuity, third-party and vendor risk, environmental risk and health and safety.

The tool covers risk identification, risk assessment, key risk indicator/metric management, loss and incident management and action management. Risks and controls can be assessed using any methodology and/or framework and aggregated into actionable risk insights and predictive analytics. Integrated content and document management systems, include version control, expiration date management, alerting, check-in/check-out, metadata management, document tagging and keywords. Internal audit management supports each step in the audit cycle, from maintenance of the audit universe to planning, preparation, reporting and finding and issue tracking.

This product features IT risk management capabilities with over 6,000 control mappings from an extensive knowledge base to map risks to requirements and automate IT risk assessments; third-party vendor risk tools that automate the lifecycle of third parties from onboarding, contracting, risk assessment, ongoing and continuous monitoring, right through to off-boarding; and business continuity and organisational resilience solutions.

The SAI360 employee-centric learning management platform and content helps organisations to deploy learning and awareness programme to mitigate the impact of people risks on the organisation.

saiglobal.com

SCAIR
INTERSYS

SCAIR is a supply chain mapping tool that helps manufacturing companies visualise their global, end-to-end supply networks. Its flow-chart driven structure allows risk and supply chain professionals to map chains, quantify business interruption losses and stress test different supply threats and recovery scenarios.

Having identified key exposures, SCAIR monitors major disruption events to provide tailored warnings of nat cats and regulatory non-compliance incidents that could impact continuity of supply. SCAIR is currently used by three of the top twelve global biopharmaceutical companies and a leading global insurer. It has also partnered with the University of Cambridge in the ReMediES project and has UKAS accredited ISO 27001 certification.

Industries that can benefit from SCAIR include medical devices, biopharmaceuticals and insurance.

supplychain-risk.co.uk

SMARTLOG
SAFESMART

Smartlog is a cloud-based fire and health and safety compliance management software tool. The core of the system is primarily made up of the following multiple compliance functions within one central 'hub'.

A Risk Assessment Tool enables risk assessments to be carried out by any competent individual along HSE guidelines. Detailed templates include Fire, COSHH, Asbestos, Legionella, Workplace Safety Inspections, Agency Workers and DSE Assessments. Custom interactive assessments can also be created and accessed by selected staff members on the system and existing templates are customisable.

20 CPD-certified courses are included, each taking 20-30 minutes on average. A digital logbook allows staff to report maintenance issues and record all related updates. All premises assessments and audits undertaken outside Smartlog can be manually logged, sorted categorically and certificates can be attached to entries. A logbook for accidents and incidents that occur in the workplace is available. Submitted RIDDOR reports can be attached to entries alongside supporting media and the progression and conclusion of a case can be logged in the system as a digital record. An Asset Management facility is for the registering, monitoring and auditing of an organisation's assets. All assets can be linked to set locations,

licences/certificates and other and any updates such as servicing, damage and repairs can be logged, detailed and timestamped.

For Policy Management, policy and procedure documents can be centrally accessible to all members of staff. Any documents that employers wish to share with their staff can be uploaded and stored in the system – such as a library of health and safety guidance forms.

Using this tool, companies can schedule site maintenance checks, fire equipment servicing, external training, PAT testing and other compliance tasks with automatic email reminders and multiple escalation levels until the task is checked off. Within an organisation, the company administrator is able to assign up to eight permission levels with varying levels of access and control – all adjustable and determined by the administrator.

Smartlog's email-driven notification system records and timestamps every user's actions so that a complete audit trail is always available.

safesmart.co.uk

STREAM INTEGRATED RISK MANAGER
ACUITY RISK MANAGEMENT

This tool allows organisations to centralise, automate, quantify and report on risk. It can be used for a variety of applications including cyber / IT risk management, enterprise risk management, operational risk management, business continuity management and vendor risk management. Aggregation and correlation features allow users to make informed decisions on the need for action, complying with regulations and standards (eg. GDPR, ISO 27001, PCI-DSS and NIST) whilst reducing the risk of breaches.

In the event of a breach, STREAM provides evidence of a diligent risk-based approach to minimise the impact of fines, reputational damage and legal costs. Additional regulations and frameworks, such as those for specific industry sectors, can be quickly and easily added into the same, single database.

STREAM can use control deployments to automatically update risk assessments to give users a full and accurate view of current exposure, both quantitatively and qualitatively. In addition, it can automate workflow to assign actions, send out notifications and alerts to users to ensure they are kept up to date on areas that need their attention. With the ability to support the Open FAIR methodology, this product provides the automation for recording, aggregation and reporting of both qualitative and quantitative risk across the enterprise whilst linking the related factors.

STREAM is a highly configurable solution which allows customisation of different roles for user-specific dashboards and permission-based viewing. Information can be viewed via standard reports, user-configurable custom reports or through integration with BI tools. Vulnerability scans, penetration test results and control metrics can be imported from external data sources. Through the use of real-time dashboards and workflow functionality, vulnerabilities are alerted to appropriate technical teams to allow for efficient remediation. STREAM has been in the market for over a decade and is available as a SaaS or on-premise deployment. It has been adopted by numerous organisations around the world, across various industries including finance, energy, healthcare, manufacturing, legal and IT companies.

acuityrm.com

SWORD OPERATIONAL RISK MANAGEMENT
SWORD GRC

SWORD GRC

Sword GRC solutions are all designed to enable the end user with powerful tools that provide a single view of risk right up to board level, empowering better business decisions and elevating risk and GRC as a new source of competitive advantage. Sword GRC's products enable collaborative working.

Sword Operational Risk Management is a feature-rich and fully web-based risk management solution designed for the finance, insurance and corporate sectors providing a flexible and easy to use tool for corporate and enterprise risk management. It provides a central fully integrated yet modular database; intuitive and easy to use solution that evolves to meet changing business demands; and individual configuration options to meet exact requirements.

A comprehensive risk register and evaluation system features an extensive range of risk models, analysis and reports which can be configured as required to meet the regulatory and business requirements of any organisation. Incidents and events can be recorded, managed and subsequently linked to relevant risks and controls to improve future management. Risk mitigation is then supported by allocated actions. For policy management and compliance, a comprehensive solution for developing, managing and evidencing compliance with corporate policies is available. Self assessment and certification can be deployed centrally or by individual business units. User-specific dashboards highlight issues and items for review or update, trends and significant changes. Another feature allows the recording of board level risk appetite statements, and a wide range of standard and custom reporting options are available.

Sword Operational Risk Management also benefits from cross-functional collaboration and alignment via the Sword GRC platform including automated processes, workflows and innovative use of visualisation tools. A powerful analytic and reporting capability delivers risk, compliance and audit information in a range of intuitive and user-friendly media that provide a personalised user experience. This tool is used by mid-tier organisations in the financial services sector, including Yorkshire Building Society, Paragon Bank, Liverpool Victoria, AON, BACS, Odyssey Re and World Bank/IEG.

sword-grc.com

SYMBIANT RISK AND AUDIT MANAGEMENT SOFTWARE
SYMBIANT

Symbiant combines risk and audit using individual modules for each task. Users can be assigned different privileges on each module which will decide what they can do and what they can see.

Modules include: Audit Universe, Audit Questionnaires, Action Tracking, Time Sheets, Working Papers, Risk Registers, Risk Library, Risk Workshops, Risk Assessments, Control Failure Simulations, Incident Reporting, Risk Indicators, Control Universe, Control Self Assessments, Risk Action Tracking and Monte Carlo.

symbiant.co.uk

VENTIV IRM
VENTIV TECHNOLOGY

Ventiv IRM allows risk, insurance, claim and safety managers to make information-based decisions on where to focus their resources, optimise the management of risk and deliver operational excellence.

It features a completely new modern user interface with easy enterprise deployment, a global search feature for comprehensive text information and document location, and an intake and workflow companion tool, Digital, for field users with responsive questioning, language, reminders, approval, delegation and full mobile support.

An embedded interactive dashboard tool allows for easy data discovery and trend identification. Integrated analytics with artificial intelligence, automated pattern detection, natural language querying and AI infused into BI. It also has the ability to integrate third-party data sets such as Census Data with Novarica data to create predictive models.

Geospatial analytics feature map search and map visualisations including with external nat cat and other location-related risk data.

Comprehensive templated reporting and analytics capabilities allow for insights and business intelligence.

A fully open architecture with REST API allows for real time integration, and a sandbox environment supports changes and testing outside of production.

Modules cover risk activity areas including: incidents and claims; safety and investigations; renewals and submissions; assets and exposures; cost/premium allocations and calculations; insurance programmes and policies, including certificates; risk engineering survey and recommendations; audits and assessments; and risks, controls, treatments.

ventivtech.com

	Origami Risk	BarnOwl	CorProfit	Coruson	Enterprise Risk Manager	Fusion Framework System	GOAT Risk	HOPEX IRM	JCAD CORE	JCAD LACHS	Maclear	Pentana Risk	Predict!	Protecht.ERM	Q-Pulse	Quantate Risk	Riskonnect	SAI360	SCAIR	Smartlog	STREAM	Sword	Symbiant	Ventiv IRM
General/admin/tech																								
Full process analysis hierarchy	•	•	•		•	•		•	•		•		•	•		•	•	•	•	•	•	•	•	•
Full process escalation hierarchy	•	•	•		•	•		•	•		•		•	•		•	•	•	•	•	•	•	•	•
Objectives hierarchy	•	•	•		•	•		•	•		•	•	•	•		•	•	•		•	•	•	•	•
Organisational hierarchy	•	•	•	•	•	•		•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•
Asset hierarchy	•	•	•	•	•	•		•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•
Financial accounts hierarchy	•				•	•		•						•		•	•	•				•		•
Expand and collapse hierarchy	•	•	•	•	•	•		•	•		•	•	•	•	•	•	•	•		•	•	•	•	•
Audit findings	•	•	•	•	•	•		•	•		•	•		•	•		•	•	•	•	•	•	•	•
Scalable and tested to 100 users	•		•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•
Scalable and tested to 1,000 users	•		•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•		•
Scalable and tested to 10,000 users	•	•		•				•			•	•	•	•	•	•	•	•		•			•	•
Context sensitive help	•	•	•	•	•	•		•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•
Screen customisation	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Search and filter	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Roll-forward capability	•				•	•		•		•	•		•	•			•	•	•		•	•		•
Multi-currency	•	•			•	•		•			•		•	•			•	•	•			•	•	•
Multi-language	•			•	•	•	•	•			•	•	•	•			•	•			•	•	•	•
Web application	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Web service API	•			•	•	•		•			•		•	•	•	•	•	•		•	•			•
Synchronisation with active directory	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Integration with MS Office	•	•	•		•	•		•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•
Integration with enterprise reporting systems	•		•		•	•			•	•	•		•	•	•	•	•	•	•		•		•	•
Integration with collaboration tools	•		•	•	•	•		•	•	•	•		•	•	•	•	•	•			•		•	
Ability to install software on users own IT infrastructure		•	•		•	•		•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	
Support for offline working and synchronisation	•	•	•	•		•		•				•	•	•	•	•	•	•		•				•
Hosted option / SaaS	•		•	•	•	•		•	•		•	•	•	•	•	•	•	•	•		•	•	•	•
Mobile capability: Add / update claims	•		•	•		•	•			•	•			•	•		•	•				•	•	•
Mobile capability: Manage tasks / activities	•		•	•	•	•	•	•	•	•	•		•	•	•	•	•	•		•	•	•	•	•
Mobile capability: View reports / dashboards	•		•		•	•	•		•	•	•		•	•		•	•	•		•	•	•	•	•
User security clearance	•			•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•			•	•	•
Technical support / service desk 24/7		•	•	•		•		•			•		•	•	•	•	•	•	•	•		•	•	•
Data management	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Load historic data	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Consolidating data from external sources	•		•		•	•		•		•	•			•	•	•	•	•	•		•	•		•
COPE data management	•					•								•			•	•			•			•
Deliver secure content	•		•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•
Integrated document scanning	•					•											•	•					•	•
Integrated electronic signature	•					•									•		•	•						•
Social collaboration and networking	•					•		•						•			•	•					•	•
Compatible with all web browsers without plug ins	•	•		•	•	•		•	•	•	•		•	•		•	•	•	•	•	•	•	•	•
Fully accessible via smartphone / tablet	•	•		•	•	•	•		•		•		•	•		•	•	•		•	•	•	•	•
Major functional areas																								
Incident reporting	•	•	•	•		•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Claims	•	•				•				•				•	•		•	•					•	•

ORIGAMI RISK

	Origami Risk	BarnOwl	CorProfit	Coruson	Enterprise Risk Manager	Fusion Framework System	GOAT Risk	HOPEX IRM	JCAD CORE	JCAD LACHS	Maclear	Pentana Risk	Predict!	Protecht.ERM	Q-Pulse	Quantate Risk	Riskonnect	SAI360	SCAIR	Smartlog	STREAM	Sword	Symbiant	Ventiv IRM
Major functional areas																								
Occurrence	•			•	•					•			•	•	•		•	•	•		•		•	•
Standard reports	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Business intelligence reports	•	•	•	•		•	•	•	•	•	•		•	•	•	•	•	•	•		•		•	•
Dashboard	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Location / Assets	•			•	•	•		•		•	•		•	•	•	•	•	•	•	•	•		•	•
Fleet	•					•				•					•		•	•						•
Internal audit	•	•	•	•		•		•			•	•		•	•		•	•		•	•	•	•	•
Assessment	•	•				•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Recommendations	•	•	•	•		•		•	•			•		•	•	•	•	•	•		•	•	•	•
Documents	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Project	•	•	•		•	•	•	•	•			•	•	•	•	•	•	•			•	•	•	•
Premium calculation and allocations	•					•				•							•	•						•
Policy	•					•	•	•		•	•			•	•		•	•		•	•		•	•
Renewal data collection	•					•				•							•	•	•					•
Insurer	•		•		•					•							•	•	•				•	•
Contacts	•		•			•		•		•	•	•	•		•		•	•	•	•	•		•	•
Health and safety hazards	•		•	•	•	•	•		•	•			•	•	•		•	•		•	•		•	•
Governance, risk and compliance	•		•	•	•	•		•	•		•	•		•	•		•	•		•	•	•	•	•
BIA	•		•			•					•			•			•	•	•		•	•		•
SCM			•			•					•			•			•	•	•		•			•
Vendor management	•					•					•		•	•	•		•	•	•		•		•	•
Risk identification																								
BCM knowledge base	•	•	•			•		•	•	•	•		•	•			•	•	•	•	•	•	•	
Issues, losses and risks	•		•			•		•			•	•		•			•	•	•		•	•		•
Custom IDs	•	•		•	•	•		•	•		•	•	•	•	•		•	•	•		•	•	•	•
Risk quantification	•	•	•	•	•	•	•				•	•	•	•	•	•	•	•	•	•	•	•	•	•
Risk comments	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•
Linked documents	•	•	•	•	•	•		•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•
Loss and accident identification	•	•	•		•	•		•	•		•	•		•	•	•	•	•	•		•	•	•	•
Linking losses to risk	•	•			•	•	•	•			•	•	•	•	•	•	•	•	•		•	•	•	•
Multiple risk types	•	•	•		•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•
Risk linkage	•	•			•	•	•	•	•		•	•	•	•		•	•	•	•		•	•	•	•
Risk review process	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•
Risk approval	•	•	•	•	•	•		•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•
Risk surveys	•	•	•		•	•		•			•	•		•	•	•	•	•	•	•	•	•	•	•
Control surveys	•	•	•		•	•		•			•	•		•	•	•	•	•	•		•	•	•	•
Risk assessment																								
Risk matrix	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•		•	•	•	•
Qualitative assessment	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•		•	•	•	•	•
Quantitative assessment	•	•	•	•	•	•		•	•		•	•	•	•	•	•	•		•	•	•	•	•	•
Gross, Residual, Target	•	•	•	•	•	•	•	•	•		•		•	•		•	•	•	•	•	•	•	•	•
Opportunity	•	•	•		•	•	•	•	•		•		•	•	•	•	•	•			•	•	•	•
Frequency	•	•	•	•	•	•	•	•	•		•			•	•	•	•	•		•	•	•	•	•

Risk Software Report 2020 – Product features

	Origami Risk	BarnOwl	CorProfit	Coruson	Enterprise Risk Manager	Fusion Framework System	GOAT Risk	HOPEX IRM	JCAD CORE	JCAD LACHS	Maclear	Pentana Risk!	Predict	Protecht.ERM	Q-Pulse	Quantate Risk	Riskonnect	SAI360	SCAIR	Smartlog	STREAM	Sword	Symbiant	Ventiv IRM
Risk assessment																								
Financial years modelling						•		•			•		•	•		•		•	•				•	•
Multiple risk impacts for single risks	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•
ROI			•			•		•	•				•	•		•		•			•			•
Escalation	•		•	•	•	•	•	•	•		•		•	•	•	•	•	•	•	•	•	•	•	•
Risk aggregation	•		•		•	•		•	•		•	•	•	•		•	•	•	•	•	•	•	•	•
Relationship matrices	•				•	•		•	•		•		•	•		•	•	•	•	•	•	•	•	•
Risk mitigation																								
Control assessment – qualitative and quantitative	•	•	•		•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•
Testing	•	•	•			•		•			•	•		•		•	•	•	•		•	•	•	•
Actions	•	•	•	•	•	•	•	•			•	•	•	•	•	•	•	•	•	•	•	•	•	•
Fallback			•		•	•		•	•		•		•	•	•	•	•	•	•		•			•
Plan	•		•	•	•	•		•	•		•		•	•	•	•	•	•	•	•	•	•	•	•
Provision management					•	•					•		•	•		•		•						•
Plans linked to multiple risks	•	•	•	•	•	•		•	•		•		•	•	•	•	•	•	•	•	•	•	•	•
Linked actions to multiple plans	•	•	•		•	•	•	•	•		•		•	•		•	•	•			•	•	•	•
Compliance auditing	•	•	•	•	•	•		•	•		•	•		•	•	•	•	•		•	•	•	•	•
Certificate management	•					•					•					•								•
Certification for projects			•		•	•					•			•		•	•	•						•
Analysis & Reporting																								
Multiple application reporting	•	•	•		•	•		•	•		•		•	•	•	•	•	•		•	•	•	•	•
Probability vs. impact diagram	•		•		•	•	•	•			•	•	•	•		•	•	•			•	•	•	•
Monte Carlo simulation		•	•		•	•			•				•	•		•		•			•		•	
Sensitivity analysis					•								•	•		•		•	•			•		
Provision management					•	•					•		•	•		•		•						•
Schedules reporting	•		•		•	•		•			•		•	•		•	•	•			•	•	•	•
Data driven reporting	•	•	•		•	•		•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•
Ad hoc reporting	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Automated email report distribution	•	•	•	•	•	•		•			•		•	•		•	•	•	•	•	•		•	•
Risk adjusted balanced score cards	•					•		•			•		•	•			•	•			•		•	
Risk adjusted GANT chart					•	•		•			•		•	•										•
Bayesian analysis			•			•							•					•						
User-defined dashboards	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•		•	•	•	•	•
Integration with business intelligence reporting tools	•	•	•	•	•	•			•	•	•		•		•	•	•	•			•		•	•
Automatic alerts	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Ability to combine data from all modules within a single report	•	•	•	•	•	•	•	•	•		•		•	•	•	•	•	•		•	•	•		•
Ability to combine data from all modules within a single dashboard	•	•	•	•	•	•	•	•			•	•	•	•	•	•	•	•	•	•	•	•	•	•
Ability to meet user reporting needs without the need from custom reports	•	•			•	•		•	•		•		•	•		•	•	•	•	•	•	•	•	•
Integration with geospatial analytics	•					•					•			•			•	•	•				•	•

ORIGAMI RISK

	Origami Risk	BarnOwl	CorProfit	Coruson	Enterprise Risk Manager	Fusion Framework System	GOAT Risk	HOPEX IRM	JCAD CORE	JCAD LACHS	Maclear	Pentana Risk	Predict!	Protecht.ERM	Q-Pulse	Quantate Risk	Riskonnect	SAI360	SCAIR	Smartlog	STREAM	Sword	Symbiant	Ventiv IRM
Analysis & Reporting																								
Automatic alerts based on the proximity and severity of external events to locations	•		•		•	•								•		•	•	•	•				•	•
Mapping capabilities	•			•		•	•	•		•				•		•	•	•	•		•	•	•	•
Drill up / down / through reporting	•	•	•	•	•	•			•	•	•	•	•	•	•	•	•	•	•		•		•	•
Download to Word	•	•	•	•	•	•		•	•		•		•	•	•	•	•	•				•	•	•
Download to Powerpoint	•	•	•		•	•		•			•		•	•	•		•	•					•	•
Export to Excel	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Incident management																								
Web-based incident reporting	•	•		•	•	•	•	•		•	•	•	•	•	•		•	•	•	•		•	•	•
Convert incidents to claims	•				•					•	•			•	•		•	•					•	•
Forward and automatically attach emails to the system	•									•				•			•							•
Automated incident investigation and escalation	•			•		•		•			•			•	•		•	•		•	•	•	•	•
Data conversion and consolidation services	•													•			•							•
Anonymous / third party incident reporting	•					•				•				•	•		•	•				•		•
Claims management																								
Full claims administration	•									•				•			•							•
Dashboards for tracking claims metrics and KPIs	•									•							•						•	•
RIDDOR / CRU1 Reporting	•													•	•		•			•				•
External claims benchmarking	•																•						•	•
Forward and automatically attach emails to the system	•									•				•			•							•
Data conversion and consolidation services	•													•			•							•
Managing financials through programme structure	•																•							•
Claim audits	•									•		•		•			•						•	•
Policy and premium management & Premium allocation																								
Insurance knowledge base										•							•							
Policy programme functionality	•														•		•							•
Policy erosion	•									•							•							•
Allocation of premiums based on exposure values and loss experience	•									•							•							•
Tracking of covered locations and perils	•									•							•							•
Ability to report on premiums by insurer, broker or business unit	•									•							•							•
Captives support	•									•							•							•
Ability to report on exposure by insurer and insurer ratings	•									•							•							•
Ability to map insurance programme	•									•							•							•
Ability to diagram policy erosion	•									•														•
Renewal data	•									•							•		•					•
Ability to customise renewal questionnaires	•											•					•							•
Automated data validation against previously submitted values	•									•							•		•					•
Automatic reminders for unsubmitted values	•																•							•
Predefined report templates for renewal data consolidation	•																•		•					•

Risk Software Report 2020 – Product features

ORIGAMI RISK

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

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

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

FUSION RISK MANAGEMENT

Fusion Risk Management
2 North Riverside Plaza, Ste. 1000
Chicago, IL 60606
USA

Tel:
US: +1 (847) 632-1002
UK: +44 (0) 20 3884 3538
https://www.fusionrm.com/
YouTube: https://www.youtube.com/channel/UCtNFz9l-0CGbyxaiRzHQ_yg
LinkedIn: https://www.linkedin.com/company/fusion-risk-management/
Twitter: https://twitter.com/fusionriskmgmt

Fusion Risk Management is a leading industry provider of cloud-based software solutions for business continuity, risk management, IT disaster recovery, and crisis and incident management. Its products and services take organisations beyond legacy solutions and empower them to make data-driven decisions with a comprehensive and flexible approach through one system. Fusion and its team of experts are dedicated to helping companies achieve greater organisational resilience and mitigate risks within their businesses.

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

Contact: Phil Walden

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

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

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

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

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

Sword GRC
1 Grenfell Road, Maidenhead, Berkshire,
SL6 1HN
Tel: 01628 582500
info@sword-grc.com
www.sword-grc.com
LinkedIn: https://www.linkedin.com/company/2229310
Twitter: @SwordGRC

Sword Operational Risk Manager (previously known as Magique) is an easy to use, fully integrated, web-based system covering Risk Management, Control Testing and Attestation, Incident/Loss Event Management, Appetite Statements and Indicators/Measures, Emerging Risks, Scenario Analysis, Policy Management and Compliance, Questionnaires and Actions.

Includes extensive email alerting, reporting and analysis through Visualisation tools.

- Configured to meet your exact methodology, terminology, workflow, security and reporting.
- Over 250 active clients from 5 users to over 1,000 users
- Mature product developed and enhanced over 20 years using proven technology
- Every implementation led by experienced Risk Management professionals
- Highly Secure – Cyber Essentials Plus Certified

Ventiv Technology
30 – 40 Eastcheap
London EC3M 1HD

Contact: Steve Cloutman

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

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

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

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

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

CIR | Risk Management

10th ANNIVERSARY AWARDS 2019

WINNERS' REVIEW

The 10th annual Risk Management Awards

Celebrating success in the practice of risk management

cirmagazine.com/riskmanagementawards

Main awards sponsor

AON

Sponsored by

BlackBerry

Regus workplace recovery

Headline partner

irm

Developing risk professionals

Supported by

airmic

ALARM embrace risk

THE INSTITUTE OF OPERATIONAL RISK

CIR Risk Management

10th ANNIVERSARY AWARDS 2019

Celebrating achievement in the sector










cirmagazine.com/riskmanagementawards

CIR Risk Management
10th ANNIVERSARY AWARDS 2019

This year's winners are

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

Risk Manager of the Year
Sponsored by Aon
Winner: Simon Cory, Nationwide Building Society

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

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

Best Use of Technology in Risk Management
Winner: Arcadis Consulting (UK)

Diversity Award
Winner: Control Risks

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

Cyber Security Initiative of the Year
Winner: Blackfoot Cybersecurity

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

Risk Management Product of the Year
Winner: Acin

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

Public Safety Award
Winner: Ecclesiastical

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

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

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

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

Major Capital Projects Award
Winner: A14 Integrated Delivery Team

Risk Management Programme of the Year
Winner: Southern Water

Operational Risk Initiative of the Year
Winner: Aviva

Risk Management Team of the Year
Winner: Nationwide Building Society

cirmagazine.com/riskmanagementawards

CIR Risk Management

10th ANNIVERSARY AWARDS 2019

International Risk Management Award (Business)

Domenic Antonucci, technical advisor, Nasir Aziz, risk and compliance director, and George M. Shaw, chief risk and compliance officer, Abdul Latif Jameel; pictured with Anita Punwani, board director, the Institute of Risk Management and awards host Zoe Lyons

Winner Abdul Latif Jameel

The judges said: Truly the gold standard in risk management, delivering tangible results at one of the most diverse companies in the Middle East.

The winning entry: Abdul Latif Jameel is a diversified business comprised of independent entities that include automotive distribution, auto parts manufacturing, financial services, renewable energy, environmental services, land and real estate development, logistics, electronics retailing and media services. Abdul Latif Jameel has an active investments arm and positions itself as a preferred business partner primarily for inward investment into the Middle East, North Africa and Turkey (MENAT) region. Established in 1945 Abdul Latif Jameel has dual headquarters in Jeddah, Saudi Arabia and Dubai, UAE, and currently has operations in 30 countries employing approximately 15,000 people from more than 40 nationalities.

Commenting on the award, chief risk and compliance officer at Abdul Latif Jameel, George M. Shaw said: "The CIR Risk Management Award offers well-deserved recognition for Abdul Latif Jameel's sustained teamwork over the past months. This success is thanks to the trust and investment placed by shareholders and governance bodies alike into its programme 'Moving up the risk maturity curve' driven by the risk team, Nasir Aziz and myself, and guided by risk technical advisor Domenic Antonucci.

"Externally, the programme has helped to strengthen the Abdul Latif Jameel brand and relationship with our stakeholders, including key strategic partners such as Toyota Motor Corporation (TMC). It also cements Abdul Latif Jameel's position as one of the leading MENAT businesses for enterprise risk management (ERM). Internally, the award further boosts engagement, especially within the network of risk management professionals at business unit level.

"Finally, the programme encourages Abdul Latif Jameel's long-term investment in risk maturity as a competitive advantage, the further expansion of the programme across the business, and helps to support key decision makers as they 'take risk, but manage it' when looking for opportunities to create value. As our markets become increasingly regulated, a solid ERM framework has supported Abdul Latif Jameel in establishing a sustainable institutional mechanism. It is an honour to have been recognised for our achievement in cementing a strong risk culture in Abdul Latif Jameel."

alj.com

Abdul Latif Jameel®

CIR | Risk Management

10th ANNIVERSARY AWARDS 2019

winner

International Risk Management Award (Business)

CIR Risk Management
10th ANNIVERSARY AWARDS 2019

Risk Management Specialist Company of the Year

Chris Andrews, head of Risk Management Solutions, Aviva; pictured with Richard Cutcher, research manager, Airmic and awards host Zoe Lyons

Winner Aviva Risk Management Solutions

The judges said: This was a tough category for this year's panel. Aviva was presented with the award for its approach of upskilling and developing its teams to offer clients a range of solutions designed to prevent losses in the first place.

The winning entry: The insurance industry has been somewhat slow to recognise that, although clients are happy to see claims being paid and normality restored following a loss, there would almost certainly have been less disruption if the loss had not occurred in the first place.

Enter Aviva's Prevention First philosophy, whereby the insurer aims to get ahead of the curve, not only providing support if the worst happens, but also offering a range of solutions designed to prevent the loss from ever happening at all. To implement this strategy, Aviva not only grew its own risk management team, but also focused on finding and developing staff with key skills relating to some of the less conventional risks around financial lines, renewable energy and cyber. The team's own development and training programme is also continuous to ensure it remains technically up-to-date. The insurer also developed a raft of products, loss prevention standards, services and innovations, with support from a Specialist Partner Network, where 50 partners provide over 100 solutions from business continuity and electrical safety, to telematics analysis and brand management.

Head of Risk Management Solutions at Aviva, Chris Andrews, said: "To win this award for the second time (we were winners back in 2017) is recognition of our prevention-first philosophy and means a great deal to the Aviva Risk Management Solutions (ARMS) team. We have an exceptional group of risk consultants who constantly strive to do the right things for our customers, working extremely hard to protect their people and businesses. They're continually thinking of new ways to innovative, manage, control and eliminate both existing and evolving risks. Our technical expertise is what separates us, so the strong focus on team development to increase knowledge and capability for our customers' benefit, is paramount. We of course won't stop here, we have some exciting initiatives in the pipeline, including a new website for 2020 to increase our reach and advice to all Aviva customers, a new drone visualisation capability and some exciting partnerships and services we're looking to develop with our customers who are always front and centre of everything we do."

aviva.com

AVIVA

CIR Risk Management
10th ANNIVERSARY AWARDS 2019
winner

Risk Management Specialist Company of the Year

CIR Risk Management
10th ANNIVERSARY AWARDS 2019

Diversity Award

Katie Murphy, senior HR coordinator, Europe and Sarah Mansour, HR director, EMEA at Control Risks; pictured with publishing director of CIR Magazine, Mark Evans and awards host Zoe Lyons

Winner Control Risks

The judges said: This firm sees its approach to diversity as a great competitive advantage, looking to foster a truly inclusive workforce as diverse as the markets its clients operate in.

The winning entry: Control Risks strives to ensure that it continues to grow and foster a diverse and inclusive environment where everyone feels valued, part of the team and that all opinions matter, reaching to the core of the company's values and its 'One Firm' culture – something it considers its biggest competitive advantage. Results of the firm's latest employee engagement survey show the firm to be a welcoming employer to individuals from all backgrounds, a workforce that treats each other with respect, and a culture that respects perspectives and opinions from people with different backgrounds.

"We are very proud to win the Diversity category at the CIR Magazine Risk Management Awards 2019! Such awards help us assess our approach and progress whilst also learning from other companies," said Sarah Mansour, HR director, EMEA at specialist global risk consultancy, Control Risks. "However, we will not stop striving for excellence now, and will therefore focus on a few new initiatives over the coming months. These include working in partnership with our two newly launched business resource groups: Mosaic, representing LGBT employees, and the Women's Network. Current activity includes global programming for 2020 and establishing workstreams. Local events, including a session in our London office led by an external coach, focused on "getting to know your personal brand" have seen the networks off to a great start.

"Our most recent global Employee Engagement Survey has also recently been closed. The results again are encouraging and include positive feedback on our culture and values with respect, inclusion and flexibility coming out as some of the highest scoring areas.

"In line with our commitment to transparency, we have just communicated the global results to employees alongside how the result will feed in to our future plans. Providing greater guidance and transparency on career development and exploring how we further support employee well-being globally are two examples."

controlrisks.com

Control Risks

CIR Risk Management
10th ANNIVERSARY AWARDS 2019
winner

Diversity Award

Public Safety Award

Faith Kitchen, education director and Nicholas Hartley, head of innovation, Ecclesiastical; pictured with James Stevenson, director of risk management, Burberry and awards host Zoe Lyons

Winner Cyber Ready from Ecclesiastical

The judges said: Ecclesiastical addresses an issue that resonates with all. Its free toolkit raises awareness of cyber issues and encourages mindful responses from kids, supporting teachers in meeting 2020 government led cyber safety lessons.

The winning entry: Keeping students safe remains a core commitment for anybody involved in the education sector. Speaking with teachers around the country, Ecclesiastical found the added pressure of new compulsory requirements in PHSE education. By September 2020, schools are required to put in place strengthened measures to protect children from harm online. Rather than providing sponsorship and generic support, the insurer sought to give teachers the tools they need to cover the cyber topic with confidence and in an engaging way. It took its proposed solution into the classroom and asked for feedback, refining the final design until it was the best it could be. By working collaboratively and iterating the solution, it has maximised relevance and take-up, ensuring that the toolkit is relevant, engaging and innovative, as well as meeting the needs of the revised curriculum.

Education director at Ecclesiastical, Faith Kitchen, commented: "We are incredibly proud to have won the CIR 2019 Risk Management Award for Public Safety in recognition of our Cyber Ready lesson plan for schools. As a leading insurer of Schools, the win means so much to us and has further validated our idea that even we thought was a little 'out of the norm' of what you might expect from an insurer! We wanted to develop something that would help schools with the risks that the digital world presents to pupils. When we carried out our research, we found that pupil mental health and wellbeing was a top concern for schools and that some of the resources in use for teaching children about digital safety, such as cyberbullying, were out of date and not appealing to the pupils. Therefore, we were keen to develop a solution that would help support teachers in delivering this important learning in a creative and engaging way."

Head of innovation at Ecclesiastical, Nicholas Hartley added: "Our next step is to have the Cyber Ready lesson plan accredited by the PSHE Association, giving it even further credibility. With this accreditation and the CIR Award, we will be able to demonstrate that we truly understand schools and their challenges and as a specialist provider of insurance and risk management we work hard to help provide solutions."

ecclesiastical.com/cyberready

Ecclesiastical

CIR | Risk Management
10th ANNIVERSARY AWARDS 2019
winner

Public Safety Award

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

For most organisations, people are both its biggest source of risk as well as one of its most important assets. An organisation's leaders and employees require careful management, both to limit the downside risks and ensure opportunities are maximised. There is a wide spectrum of people-related risks, most of which are not currently managed as effectively as possible. According to new research published by Airmic, people risks are typically managed in siloes, with little cooperation between risk management and human resources, leading to inefficiencies and missed opportunities. These include the failure to attract or retain talent as effectively as possible; less-effective safety standards and cost inefficiencies. The research calls for a more integrated approach to people risks, with greater collaboration across business units, especially risk management and human resources. The benefits are clear and mutual. HR has the data to provide greater insight into the organisation's workforce, while the risk professional should be able to identify insurance solutions, particularly in the area of healthcare and employee benefits, that will strengthen HR's offering to employees while containing costs.

Organisations are entering an era of increased volatility with regards to workforce issues. Britain's departure from the European Union, for example, will impact organisations' ability to retain and attract talent. Political unrest in regions that are typically peaceful is also on the rise; protecting employees from violence abroad is becoming a greater challenge.

Looking domestically, the changing demands and expectations of a growing millennial workforce is affecting businesses, and those that don't adapt could lose out in the battle for talent. Meanwhile, providing employee benefits and healthcare to employees is becoming more expensive, with medical insurance escalating at a CAGR of almost 10% a year globally. These are far-reaching challenges that can only be tackled with cross-business support. For risk professionals looking for opportunities to take risk out of its silo, people risk is a good place to start.

John Ludlow is chief executive officer of Airmic

In association with airmic

Firstly, as this is my inaugural column for CIR, I'd like to thank outgoing chairman Socrates Coudounaris for his unerring work in this post over the last couple of years. I am in the fortunate position of being able to build on the good work done by the CEO, staff and the immediately preceding chairs in stabilising the Institute's financial position, building a strong board and starting the next phase of our growth. We are now in a position where we can capitalise on that financial strength to drive towards fulfilling the Institute's vision.

As such, my four priorities include a focus on the heart of the Institute – in particular, qualifications, training and thought leadership, really fulfilling our role as the pre-eminent global risk management body; the integration of the Institute of Operational Risk, which joined the IRM group in 2019; the exploration of whether now is the right time to move to a 'professional' chairman, having received members' approval to change the Articles at the 2018 AGM; and leading the board in exploring whether it is right to move the IRM to charitable status, which would naturally involve membership approval.

The Institute is at an exciting time in its history, where we can look forward and really make our mark. We will be increasing the diversity and content of our product portfolio, in both qualifications and training. I am particularly keen to continue to operate and expand in international markets. I aim to lead the board with vigour and commitment through this next stage. During Socrates' term we have gone from strength to strength and I'm looking forward to continuing his good work and playing a key part in professionalising risk management globally. And, in addition to the leading qualifications in ERM in the insurance sector, the IRM International Certificates, we have also launched our new Supply Chain Risk Management Certificate – developed with the Supply Chain Risk Management Consortium. The qualification provides a broad understanding of supply chain risk management principles and practices – a valuable asset in any risk managers toolkit.

Iain Wright is chairman of the Institute of Risk Management

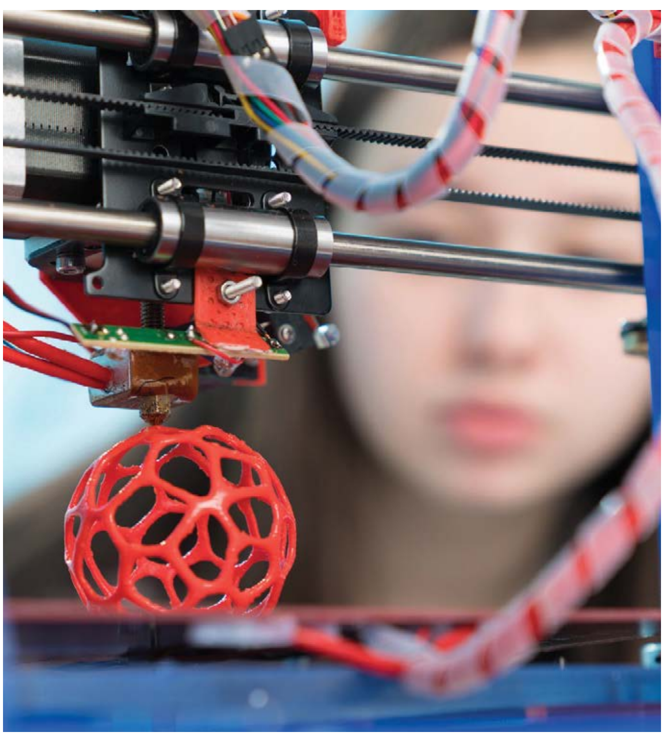
In association with irm

2020 Predictions: No rest for the wicked

Class actions, climate adaptation and workplace modernisation are amongst the challenges the insurance sector can look forward to this year, according to a major study just conducted by DAC Beachcroft

In the run up to the New Year, CIR's popular annual predictions series was once again amongst the most read on our website. So, for the last page of our first issue of the year, we thought it fitting to bring you some more insight into what's in store, this time from law firm DAC Beachcroft, which recently published over 80 such predictions for the global insurance market.

Amongst the forecasts, a feature of the US legal system for years, the momentum behind class actions is picking up speed, it warns. In product safety, liability and recall, for instance, it says insurers will need to ensure that insureds involved in the manufacture or use of 3D printers are providing adequate warnings and risk assessments to make sure this technology is used as safely as possible, especially as use extends into schools and homes. Studies report links to adverse health conditions including asthma and cancer, with the printing producing high amounts of ultrafine particles and volatile organic compounds while in use (potentially for extended periods of time), which can pass through the lungs and travel to other organs and also transfer toxic material into the body.



Meanwhile, from discrimination and mental health issues to health wearables, workplace modernisation is a significant industry issue. Within professional liability, for example, the law firm warns that solicitors' conduct could come under scrutiny this year, as the #MeToo campaign has increased the Solicitors Regulation Authority's focus on tackling misconduct and harassment.

"Regulatory obligations of integrity and maintaining public trust in the profession are the hook on which such matters can lead to disciplinary investigation. The well-publicised sexual misconduct case of SRA v Ryan Beckwith resulted in a £35,000 fine and adverse costs of £200,000 despite the absence of a criminal conviction or a finding on the issue of consent. Some commentators have questioned whether the SRA's approach is proportionate. With a further 25 cases of alleged sexual harassment and misconduct to be heard, the profession faces a difficult 12 months and firms should ensure they have robust procedures in place to deal with such behaviour," the report states.

"Insurers will need to ensure that insureds involved in the manufacture or use of 3D printers are providing adequate warnings and risk assessments"

On the theme of climate change, the firm's experts examine underwriting the unknown in renewable energy; the growing impact of climate risks on coastal areas in Australasia; the use of parametric policy triggers; and the need for early recognition at board level that all firms are vulnerable to risks associated with climate change – whether or not they are operating in an environmental sector. It also talks about the PRA's regulatory focus on the issue.

Staying with the climate theme, Duncan Strachan, partner in the firm's international casualty team, highlights the German court's consideration of the case of a Peruvian farmer's claim against RWE for the alleged impact of its emissions on farming.

"Regardless of the outcome, we expect to see a surge in climate change-related litigation," he said. "State-owned companies in the fossil fuel industry are at heightened risk, particularly in Latin America and South East Asia, where there is broad recognition of the right to a healthy environment. Class actions are a critical issue for the international insurance market and DAC Beachcroft's global reach enables us to take a true barometer reading across all jurisdictions."

Technological, geopolitical and legal developments also feature among the law firm's predictions for this year.

Written by Deborah Ritchie

BUSINESS CONTINUITY SOFTWARE

ClearView Continuity
Astral House
Granville Way
Bicester
Oxfordshire
OX26 4JT

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

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

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

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

ClearView – we make the complicated simple.

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

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

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

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

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

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

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

BUSINESS CONTINUITY SOFTWARE

BUSINESS CONTINUITY, DISASTER RECOVERY & ALWAYS ON INFRASTRUCTURE

BUSINESS CONTINUITY, LOGISTICS

CMAC Business Continuity Transport
The Globe Centre, St James Square,
Accrington, Lancashire BB4 0RE

Contact: Ashley Seed

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

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

CLAIMS HANDLING & 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
www.jcad.co.uk
Twitter: @jcad2

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

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

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

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

CLAIMS HANDLING & RISK MANAGEMENT SOFTWARE SOLUTIONS

ORIGAMI RISK

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

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

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

---

ventiv TECHNOLOGY

Ventiv Technology
30 – 40 Eastcheap
London EC3M 1HD

Contact: Steve Cloutman

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

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

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

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

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

WORK AREA RECOVERY

Fortress

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

Tel: +44 (0)20 3858 0099
info@fortressas.com
www.fortressas.com
Twitter: @fortressas
LinkedIn: https://www.linkedin.com/company/fortress-availability-services-limited

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

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

Our services span:

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

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


Different by design
The only SaaS platform to provide integrated solutions to the entire insurance value chain: Risk Managers, Brokers, TPAs, and Insurers
ORIGAMI RISK
info.origamirisk.com/CIR-2020