



airmic

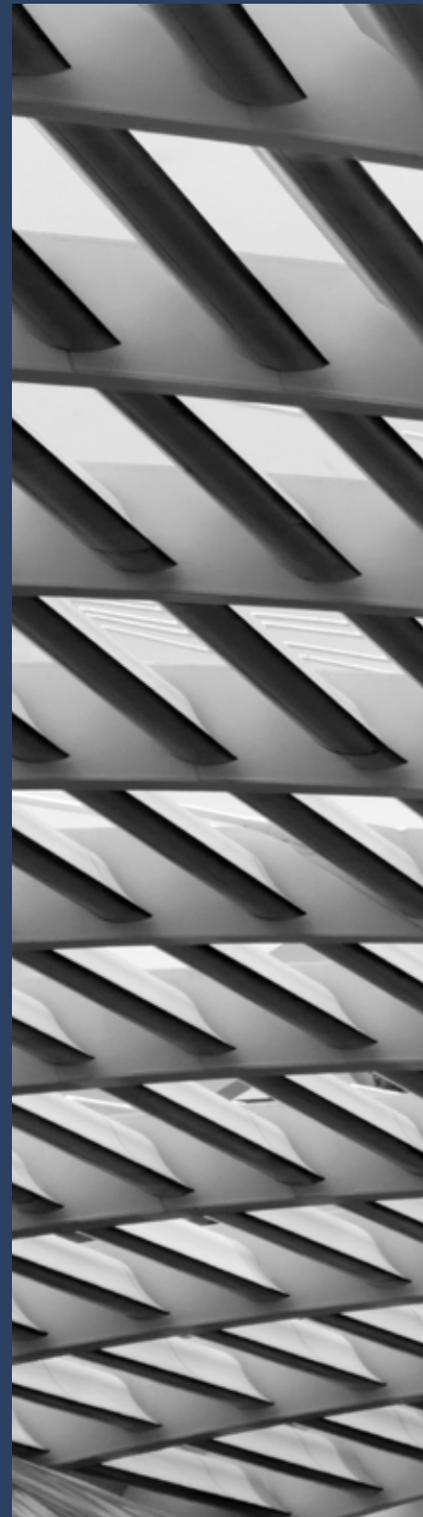
Top risks and
megatrends
2020

Airmic annual survey report



Contents

Forewords by: Airmic, AIG, Control Risks, KPMG, QBE, Willis Towers Watson	4
Executive summary	9
1. The profession	10
2. Top risks today	16
3. Nightmare headlines	20
4. Risks and megatrends: a. Cyber & technology b. Climate & environment c. Trust & reputation d. Geopolitics & populism e. Governance, laws & regulation	22
5. Resilience in an unpredictable year	38
6. Insurance faces a seismic shift	42
Conclusion	47
Annex: Research & survey methodology	48





In the Covid-19 context, great leadership fuelled by managerial agility were key factors in managing an effective response, not plans gathering dust with inert responses that took too long to ignite.

Foreword

Airmic

As we entered the year, risk professionals may have been kept awake at night thinking about cyber risks, perhaps coloured by outstanding uncertainties surrounding Brexit and issues associated with climate change. How much difference a few months have brought. With the Covid-19 pandemic, there has been unprecedented disruption to businesses and daily lives not seen for decades.

Disease is a known risk and has been on risk registers for many years and some organisations had prepared extensively for a pandemic, but the scale and velocity of the spread of Covid-19 took many by surprise. In this context, great leadership fuelled by managerial agility were key factors in managing an effective response, not plans gathering dust with inert responses that took too long to ignite. But however well leaders performed, or teams responded, organisations continue to grapple with uncertainty.

Airmic's survey report for 2020 highlights the risks and megatrends impacting organisations and provides the context in which risk professionals are operating. The report walks us through how we can navigate five risk megatrend areas and their connectivity, and the effect of a crisis such as the pandemic on other risks. Finally, the report looks at how insurance buyers, brokers and insurers should work together – especially during times of crisis. I would like to thank our survey partners – AIG, Control Risks, KPMG, QBE and Willis Towers Watson – who have provided their insight to the survey conclusions and their thoughts on specific megatrend areas.

Risk professionals must be dynamic in stakeholder engagement. A more creative and collaborative approach to managing risks and opportunities will enable them to recognise and address institutional and individual biases, learn from others who have different attitudes to risk, context and experiences, and discover blind spots. This will help them to surface emerging risks and opportunities for which evidence may be limited or conflicting.

The pandemic has upended work and life as we know it. It has changed the profile of risks we were familiar with and created new risks and new opportunities. Research tells us that during previous pandemics, the level of innovation was proportional to the level of disruption they caused – so now is a vital period for innovation and seizing opportunities to innovate, not retreat.

Julia Graham
Deputy CEO and Technical Director
Airmic





Organisations are facing extremely turbulent times. Risks in relation to governance, laws and regulation continue to be of significant concern to risk professionals and their organisations.

Over the medium term, that includes compliance with evolving digital regulations – a sign of the importance of cyber and technology risks.

Through our directors and officers (D&O) claims notifications, we see that scrutiny of the decisions made by boards and management is intensifying.

At this time of writing, regulatory uncertainties related to Brexit persist as both the UK and the European Union have still to reach an agreement on several aspects of their relationship after the period of transition.

Meanwhile, the current environment may distract from risks relating to sanctions, regulatory activity, trade tariffs, bribery, corruption and anti-money laundering, but these risks continue to have material implications for boards and risk professionals.

Businesses that are informed enough to anticipate threats, prepare for them, stress test and adapt accordingly will be best placed to persevere in this climate. This requires strong corporate governance and robust enterprise risk management that gives organisations room to innovate while managing the risks of their ongoing business.

This is where D&O insurance is a key component of a company's risk management strategy, enabling, as well as protecting, directors and officers.

We are delighted to have collaborated on this report with Airmic, with whom we have worked on a series of publications on D&O liability since 2018. We hope this latest instalment will inform those involved in the purchasing and usage of D&O insurance, and provide a timely update on the situation more generally and on risks relating to governance, laws and regulation.

Géraud Verhille
Head of Financial Lines
AIG UK



Control Risks

If anyone doubted the importance of digital transformation to business, Covid-19 has underlined that reality with a vengeance. Our new virtually enabled homeworking arrangements have transformed the daily reality for millions of employees, while also increasing our vulnerability to cyber-attacks.

Meanwhile, the targeting of cloud service providers and software supply chains continues to raise the spectre of cascading attacks that flow through the systems of global companies, and their suppliers, at unprecedented speed.

Regulatory risk is also a growing challenge. As seamless global connectivity has grown in recent years, so conversely has the emergence of a fragmented regulatory backdrop.

Politics only complicates this backdrop. Tensions between the US and China, and the rise of protectionism in the creation and trade of software and hardware are catching global companies in the crossfire.

Organisations can prepare themselves for these emerging challenges in the coming years through further investment in highly automated security operations and intelligence centres. Nevertheless, the critical success factor in any digital transformation programme is to ensure it is focused on people. Technology is a crucial catalyst in the process, but investment in skills and culture is a much more sustainable way of building a secure, compliant and resilient business in the digital age.

In the 50 years that Control Risks has supported clients across the globe, the political, technological, environmental and societal landscape has changed beyond all recognition. This has created wealth and opportunities, but also conflict and uncertainty.

Against this backdrop, Control Risks embarked on this study with our partners at Airmic to better understand the threats of the changing world. We hope in turn that this report will be of value to all those seeking to enhance their understanding of risks and megatrends, towards better decision-making.

James Owen
Partner, Head of Cyber Security
Practice, EMEA
Control Risks





Trust and reputation have become increasingly important to businesses. This has come at a time when social media brings with it a growing propensity for amplifying reputational damage, especially following activist events such as #MeToo, while the phenomenon of fake news and disinformation campaigns is also impacting businesses and organisations in very direct ways.

The Covid-19 crisis has put businesses and organisations under more stress than ever, during which mistakes may be made, inadvertently or otherwise. One might think that businesses may be more easily forgiven for their errors given the context, but consumers continue to find many corporate transgressions unacceptable.

All of this comes as traditional shareholder value is increasingly being replaced by broader stakeholder value, which places greater weight on intangible assets like reputation. This means that organisations are required to manage broader critical trade-offs and critical risks, which makes the risk landscape increasingly complex.

We see reputation playing an increasingly important role as a major driver of corporate value across industries. Businesses that will go beyond focusing on their capabilities and will start proactively managing their character will have higher reputational value. That will have a direct positive impact on financial outcomes, customer loyalty and advocacy, and employee job satisfaction. Genuine care about reputation is no longer optional, but an essential part of long-term business success.

As a risk management community, Airmic represents the customer of the commercial insurance market. At KPMG, we see the customer driving many of the strategic decisions for insurance carriers and distribution partners. We are therefore delighted to collaborate with Airmic on this report, which examines the risks and megatrends impacting risk managers and their organisations.

We hope you find some helpful guidance for how you might challenge yourself and your traditional role profiles to increase the value you bring to your business.



Paul Merrey,
Strategy Partner
KPMG

Ben Harris, London
Market Director
KPMG

Arturs Kokins,
Associate Director
KPMG



The world is in a very different place now than when Airmic members were asked about the risks that most concerned them.

Impacts of Covid-19 will be felt across each of the megatrends outlined in this report. In 2019, QBE ran a programme of research which empirically proved that the world was increasingly unpredictable. Our research spanned the megatrends elaborated in this report and while there were certainly peaks and troughs in certain pillars, one resounding truth was the interconnectivity of factors. Megatrends do not exist in isolation, they perpetually change and are changed by one another.

In response, companies need to take a critical look at where risk management fits into the board level agenda. Is it a tick box exercise or a core part of the strategic agenda? Risk management has a critical role to play in assisting companies with growing unpredictability. Questions companies and their boards might wish to ask themselves are:

- How much time and focus do the senior executive teams and board spend on understanding, assessing and discussing risks through the year?
- Is the time spent discussing risks and mitigation strategies commensurate with the potential impact of that risk?
- If not, why not? To what extent is the team's thinking more or less influenced by frequency than severity? What would one have to believe for a risk and associated scenarios to become a reality? How are short-term and long-term dynamics managed?

The thought process triggered by the above questions might inform the psychological elements that may be, often unconsciously, shaping the risk discussion and where it sits on a senior team's agenda as well as inform different and better approaches.

Increased volatility and uncertainty will require a more in-depth conversation around risk, supported by modelling, scenario planning and more granular information.

Risk will not go away, but it will change. The best we can do is be informed, prepare and be resilient.



Cécile Fresneau
UK Executive Director,
QBE

Willis Towers Watson

While the Covid-19 pandemic is primarily a problem of human health, it has carried inevitable consequences for geopolitics as well as domestic politics. After all, geopolitics is about how businesses sit within the economy, policy and geography, and the impact that events like pandemics have on this relationship.

If organisations can pre-empt the changes in the way businesses and the economy will operate in the ensuing six to 12 months, they can move from reacting into strategic planning. This will help to gain competitive advantage in the new normal and improve resilience. This is essential because all the other risks don't go away – cyber-attacks, floods, earthquakes, terrorism incidents could all still occur.

It isn't all negatives – the Covid-19 experience may bring opportunities such as the opportunity to evaluate different and more cost-effective ways of working, build a more resilient society, larger home markets and establish more reliable supply chains.

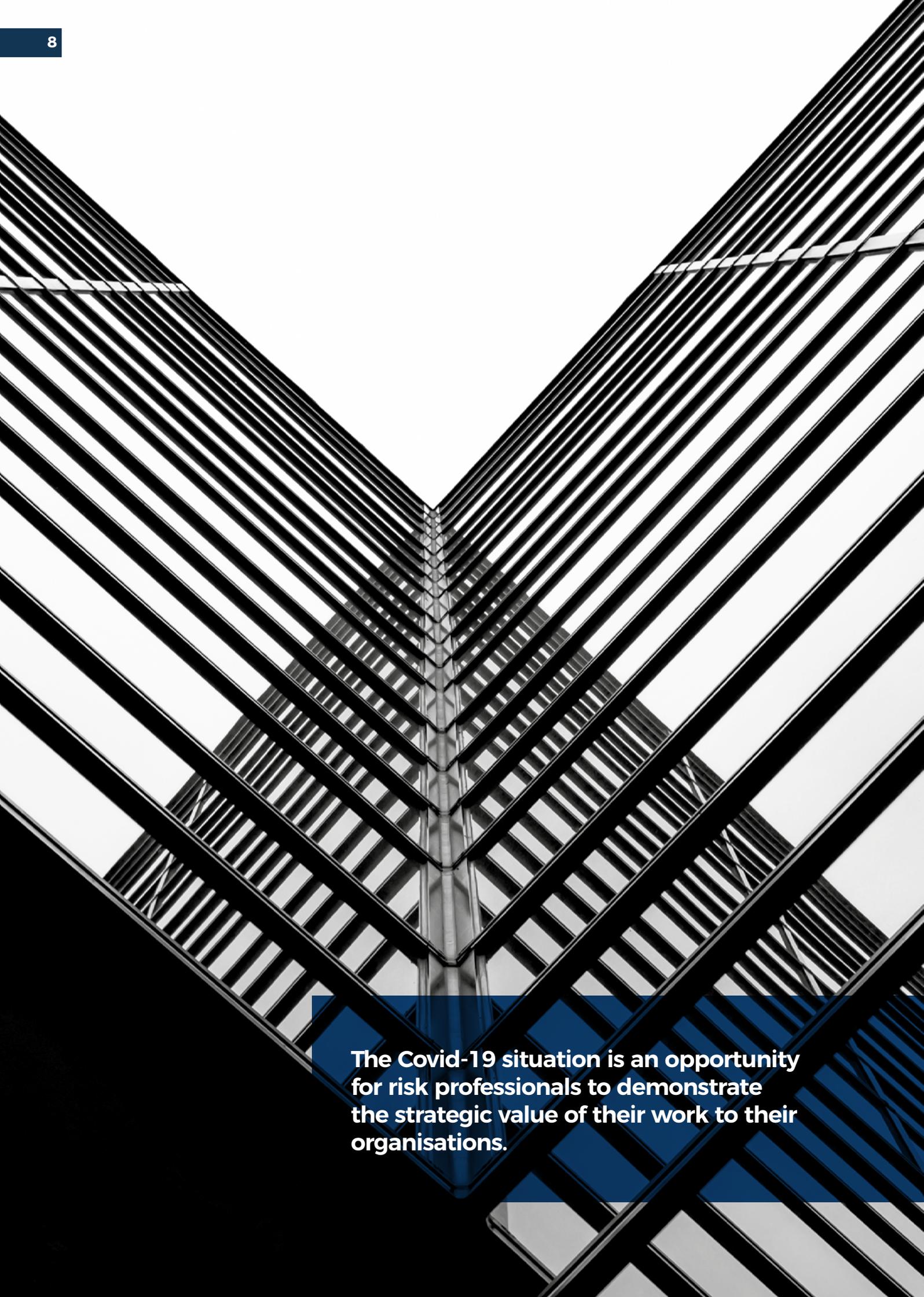
Whatever the size of your organisation, geopolitical circumstances demand a high degree of engagement and understanding. Risk professionals need to be able to identify and understand geopolitical risks, their drivers and the connections between them, so they can mitigate the risks and seize new opportunities.

Different functions within businesses also need to look at these connected risks collectively and manage them using an integrated approach. They need credible and up-to-date information and relevant risk insight and analytics to see the potential impacts to their business. Risk leaders need to speak to their CEOs and boards about geopolitical risk.

With this in mind, Willis Towers Watson collaborated with Airmic on this study on risks and megatrends. We hope you will find this report useful.

Neal Croft
Global Client Relationship Director
Willis Towers Watson



The background of the page is a complex, abstract geometric pattern. It consists of numerous thin, dark lines that intersect to form a series of overlapping, nested V-shapes. The lines are arranged in a way that creates a sense of depth and perspective, drawing the eye towards the center. The overall effect is a dynamic and modern architectural or structural design.

The Covid-19 situation is an opportunity for risk professionals to demonstrate the strategic value of their work to their organisations.

Executive summary

Airmic conducted its annual member survey from 14 February to 31 March 2020, enhanced by qualitative input from Airmic member roundtable discussions and observations from organisations that are stakeholders in the management of risk.

- As the UK went into lockdown, **risk professionals were most concerned about the risks of business interruption following a cyber event**, followed by the **loss of reputation and brand value** – the same top two risks they were concerned about last year. **Diseases and pandemics** per se featured in fourth place among their list of concerns this year.

- The Covid-19 situation is an opportunity for risk professionals to demonstrate the **value of their work to their organisations**. They are having more contact with their senior management and are more firmly embedded in what their organisations are doing.

- Risk megatrends:

- Individual and corporate exposure to **cyber threats** is expanding at a rapid rate. Artificial Intelligence techniques, while still in their infancy, are being utilised in more state and criminal operations for faster and harder-to-detect attacks. Targeting of operational technology is increasing as outdated analogue systems digitise and converge with IT networks at corporate headquarters.
- Businesses will bear the brunt of **climate change**. These will cause knock-on effects that will disrupt supply chains and impact staff, ultimately leading to lost revenues and reputational damage. Yet many businesses still see climate action as external to them – something for governments instead to deal with.
- **Trust and reputation** have become increasingly important to businesses. With the pandemic, all businesses and organisations have been placed under additional stress. One might think they may be more easily forgiven for their errors, but consumers continue to find many corporate transgressions unacceptable.
- The nature of risks today, especially **geopolitical risks**, is that they are increasingly interconnected. Indeed, while much has changed, there is a surprising element of continuity in the geopolitical threats that companies face in the Covid-19 era.
- Risks in relation to **governance, laws and regulation** continue to exhibit a significant level of concern for risk professionals and their organisations.

The Pandemic

- > Even before the pandemic struck, the writing was already on the wall – 2020 was set to be a year of heightened **unpredictability**. The pandemic has brought uncertainty to a whole new level. Many of the emerging challenges, such as mitigating the effects of climate change or protecting complex digital supply chains, will require organisations to work in partnership and build **collective resilience**.
- > **The lack of adequate insurance cover, at an affordable premium, is emerging as a risk in itself**. The majority of businesses are exploring alternative risk transfer solutions, including new and greater use of captives, for their 2020 renewals. Over a third of respondents plan to invest more in risk management solutions.

Insurance

- > **The insurance industry is at the crossroads**. The hardening market is already forcing businesses to look at alternative transfer options, and an ill-judged response to the pandemic could detonate the whole mix.
- > It is **in the interests of insurers, brokers and insurance buyers to work together** openly and constructively, particularly at this time of the Covid-19 crisis.



The profession

Who are Airmic members?

Airmic’s members hold leading positions in the risk profession, among some of the largest businesses in the world. Just over half of respondents are heads of risk management or insurance for their organisations, with a responsibility for the purchase of insurance. A majority come from organisations with a global turnover of £1 billion to £10 billion and beyond, while 34% are from organisations with more than 25,000 employees.

They are also evenly spread across a range of sectors. Members in the insurance, banking and financial sectors earn the highest salaries among respondents, with 42.8% of respondents in this combined grouping earning an annual salary of more than £120,000. Those from other sectors such as construction and civil engineering, and food and drink, are among the respondents who draw some of the highest incomes.

There is a growing pipeline of female talent. Younger risk professionals are more likely to be female, while the gender

balance among those with up to 15 years in the profession is almost perfectly equal. This broadly continues the trend in the profession picked up in an earlier Airmic study on the future of the profession, which was released in March 2020.

Working with boards and senior management

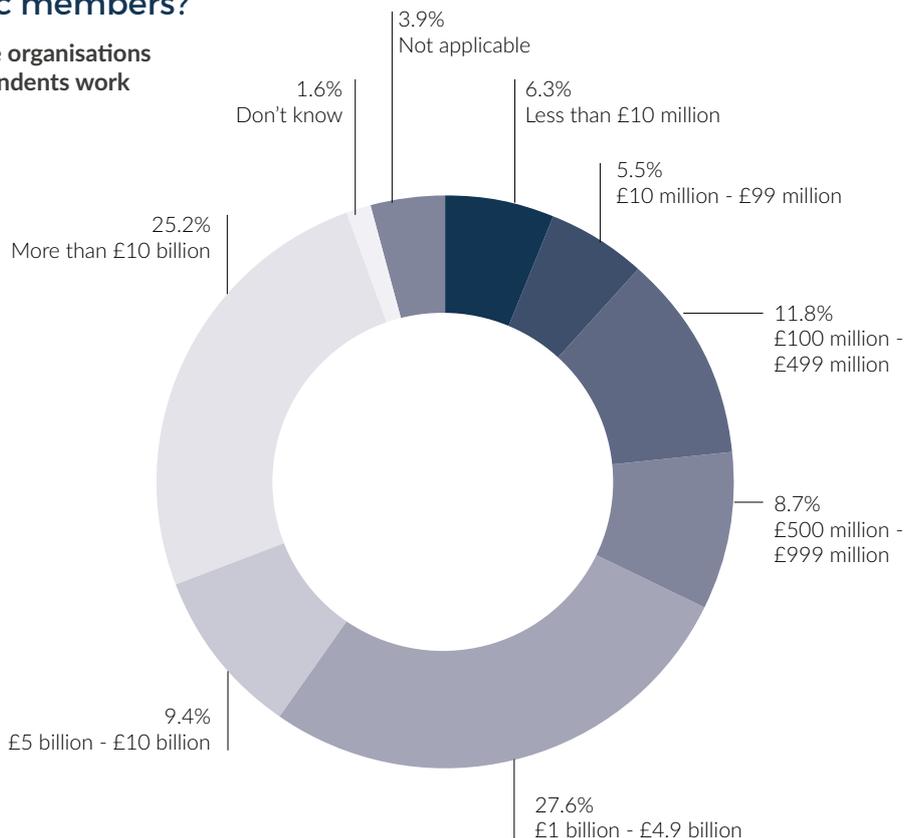
In the coming years, the Airmic survey will include other measures of diversity such as ethnicity and sexual orientation.

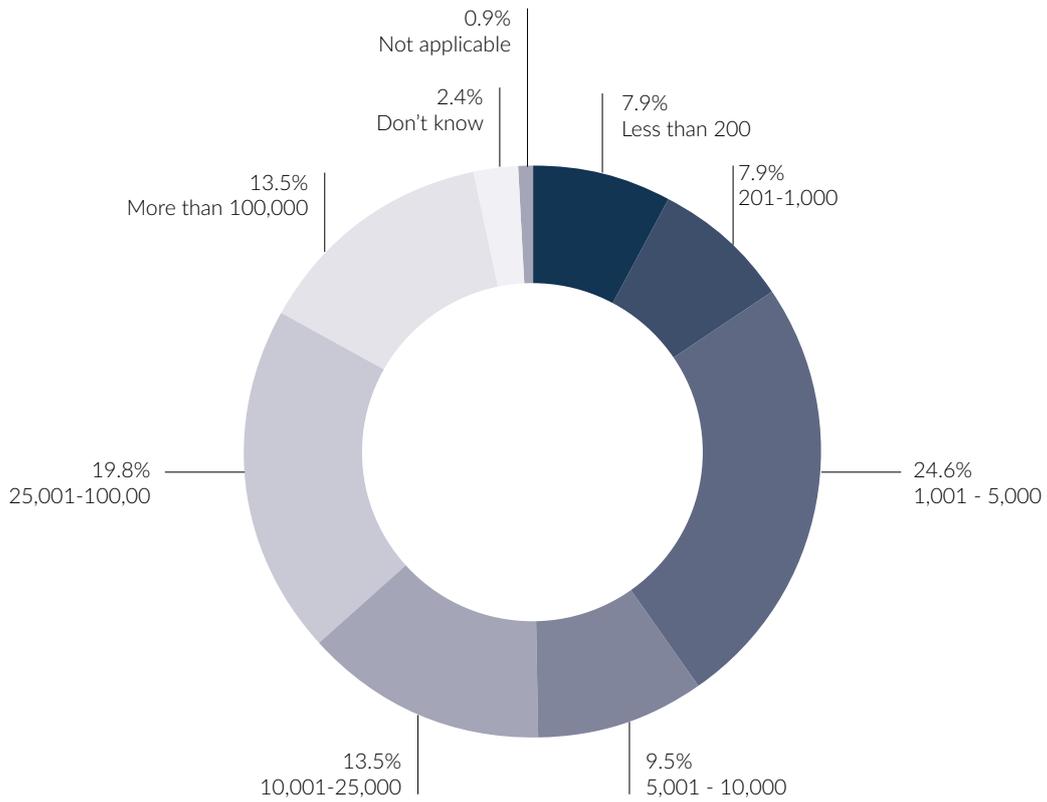
Our risk professionals work closely with the boards and senior management of their organisations. Among them, 40.2% make formal presentations and present papers to their boards regularly, while 66.9% do so for their senior management. More than eight in ten of their organisations have a risk committee.

Among our risk professionals, 59% report greater collaboration across all functions. A further 20% say that they are becoming the point for aggregating risk-related information from the other functions in their organisation.

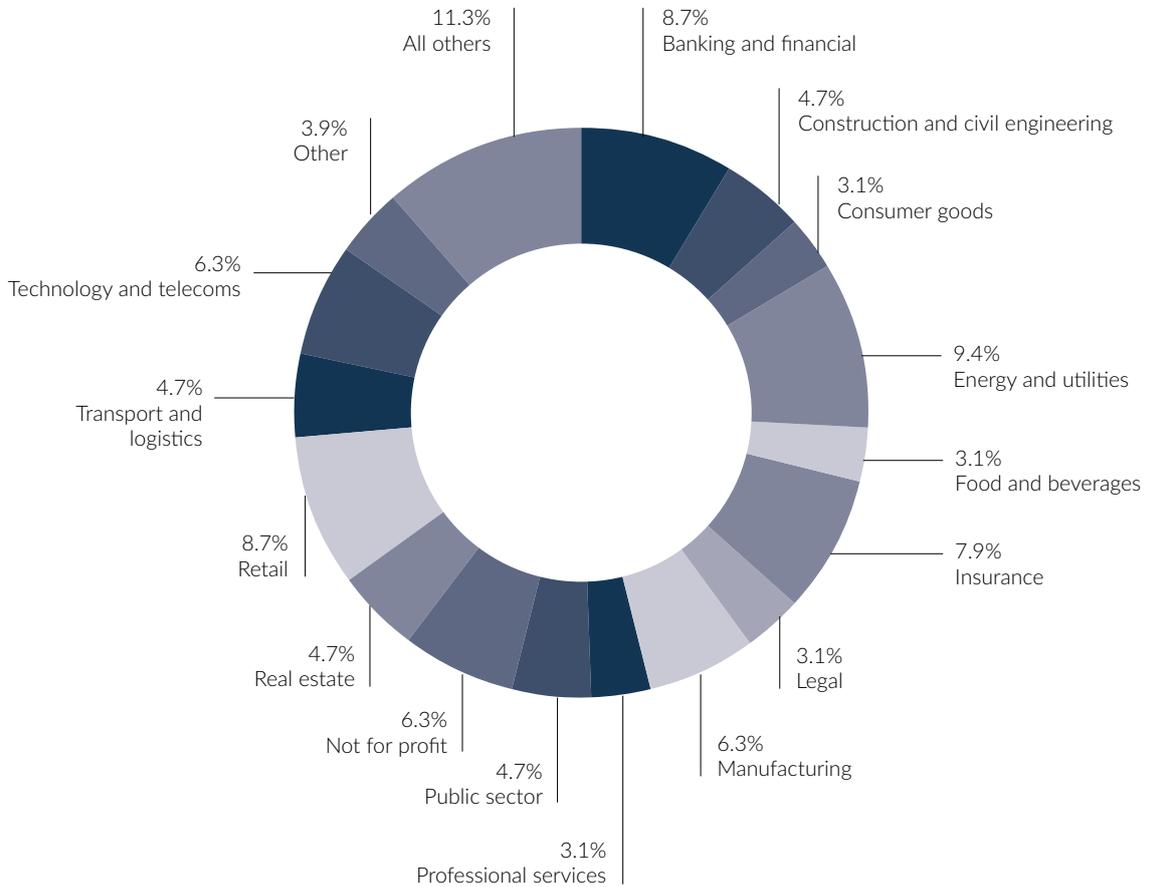
Who are Airmic members?

Global turnover of the organisations in which survey respondents work

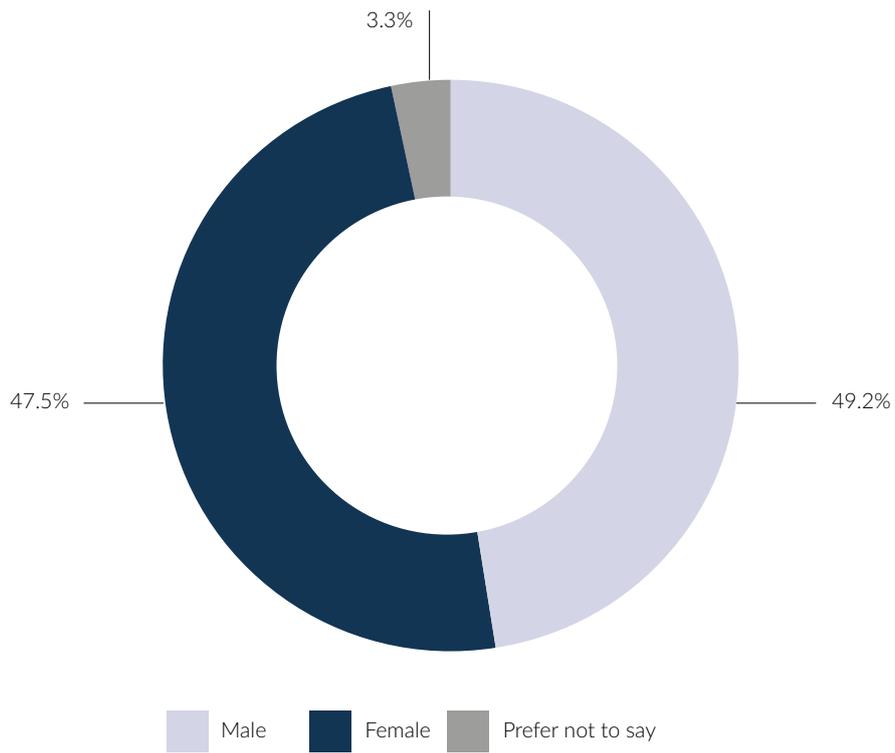




Total number of employees globally of the organisations in which survey respondents work



Sectors in which survey respondents work



Risk professionals with up to 15 years of experience, by gender



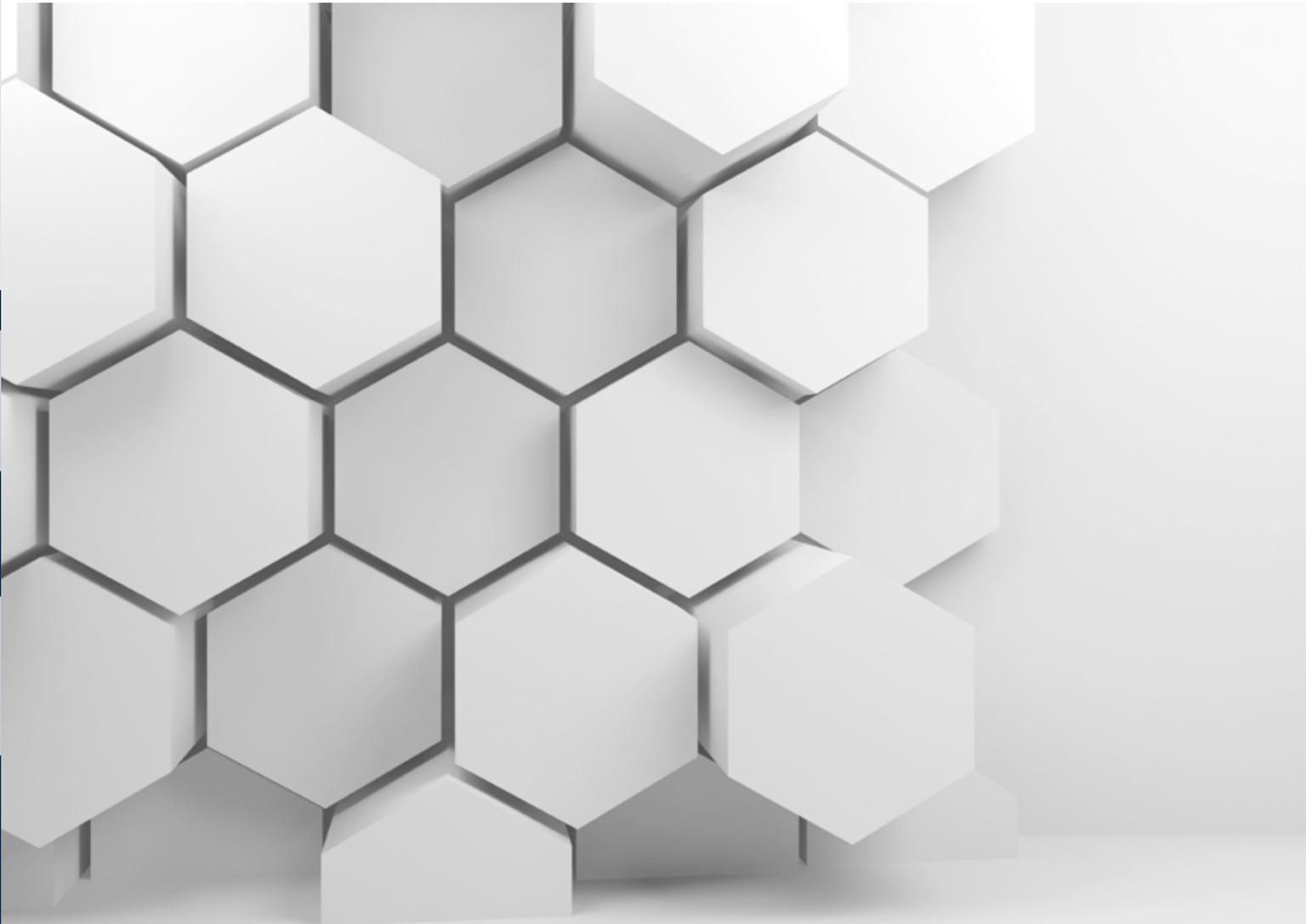
Technology use

Nearly half of all risk professionals now use data analytics in the course of their work and over 40% use cloud computing. A small minority use more cutting-edge forms of technology such as Artificial Intelligence, including machine learning and blockchain.

Among risk professionals, the perception is that what generally holds back organisations from adopting new technologies and processes is the investment needed. A sizeable number also say it is due to the perceived lack of added value from using them.

The work-from-home arrangements, necessitated by the Covid-19 lockdowns, have led to the rise of the 'remote risk professional' – they have to be professionally agile while continuing to collaborate more closely with the other functions

in their organisations, particularly in times of crisis. This goes beyond being able to use video conferencing platforms, which will be *de rigueur* as we enter the post-Covid-19 new normal. Risk professionals need to be prepared for cultural and professional change, and mesh technological fluency together with their traditional technical risk competencies. This will position them to help steer their organisations in negotiating today's dynamic and complex risk environment.



Spreadsheet (e.g. Excel)	96.9%
Data analytics	48.8%
Cloud computing	42.5%
Robotic process automation (RPA)	4.7%
Artificial Intelligence (including machine learning)	5.5%
Data visualisation	17.3%
The Internet of Things (IoT)	7.9%
Blockchain	1.6%
Risk management information systems (RMIS)	43.3%
Other	2.4%

Technologies and processes used by risk professionals in their work

The investment needed	64%
The level of skills within your department to use them	32.3%
Resistance to change internally by your department	8.7%
Resistance to change internally by your organisation	26.8%
The perceived lack of added value from using them	45.7%
Regulatory and legal uncertainty	10.2%
Consumer sentiment	1.6%
The level of digital maturity in your organisation	33.9%
Control over tech investment	20.5%
Other	7.9%

Obstacles to the adoption of new technologies and processes



2

Top risks today

The Covid-19 pandemic is a public health crisis. Because of the interconnected nature of risks today, however, the crisis has also manifested itself through a range of other risks for businesses.

Connected risk, as defined by the Russell Group, is the systemic exposure of commercial organisations, their partners, suppliers and clients to cumulative and cascading financial, operational and reputational vulnerabilities. Due to globalisation and digitisation, perils as varied as cyber-attacks, disinformation campaigns and pandemics are compounded when they connect to each other, resulting in threats to the balance sheets and operations of the insurance community and their corporate clients.

As the UK went into lockdown by the end of March 2020, risk professionals were most concerned about the risks of business interruption following a cyber event, followed by the loss of reputation and brand value – the same top two risks they were concerned about last year. Diseases and pandemics per se

featured in fourth place among their list of concerns this year.

Cyber risk has loomed large as a front-of-mind risk occupying risk professionals for some years. This has clearly intensified during the pandemic, as a vast swathe of employees began to work from home and access to important data was no longer restricted to the more secure environment of offices.

Political uncertainty had kept risk professionals up at night for much of last year, given its propensity to bring about unexpected regulatory and legislative changes, or cause disruption to supply chains. The geopolitical situation in the past few years has also been especially tense and volatile. That has now taken a back seat as an issue of direct concern, though risk professionals should not underestimate how the challenges and frustrations of the pandemic could wreak havoc politically in the near to medium term. This is further explored in the megatrends section of this report on geopolitics and populism.

2020 Ranking	Risk	2019 Ranking	Risk
1	Business interruption following a cyber event	1	Loss of reputation and/or brand value
2	Loss or theft of personal data	2	Business interruption following a cyber event
3	Failure of operational resilience	3	Political uncertainty
4	Disease and pandemics	4	Changes in regulation
5	Loss or theft of personal data	=5	Failure to attract and/or retain talent with the right skills
6	Supply chain failure	=5	Loss or theft of personal data
7	Changes in regulation	7	Supply chain failure
8	Failure to attract and/or retain talent with the right skills	=8	Changes in consumer behaviour
9	Changes in consumer behaviour	=8	Competitor business models fuelled by digital transformation
10	Political uncertainty	=8	Uncertain economic growth

Top principal risks and impacts for risk managers and their organisations today (2020 vs 2019)

Emerging risk management

The pandemic is a high impact, low probability emerging risk. Such risks do make it onto a risk register but often fade into the background when risk severity is considered as a combination of impact and probability.

Managing emerging risks cannot be a strategic afterthought. Provision 28 of the UK Corporate Governance Code 2018 requires boards to undertake a “robust assessment” of their organisation’s principal risks, including risks that result in events that may threaten the organisation’s business model, future performance, solvency and reputation. Risk professionals are integral in supporting their boards in this role.

Globalisation and an increasing emphasis on cost optimisation have resulted in more complex supply chains with larger footprints. Natural disasters or other events that take place far away from the organisation’s core business and properties can have a significant impact on operations and bring the organisation to a halt.

However, the code continues to focus more on audit and less on positive risk-taking. There is a danger that boards will spend too much of their limited time on more traditional risks at the expense of emerging risks. Clearly, organisations cannot compress everything onto the board agenda, but there needs to be a balance that allows for informed discussions, decision-making and communication about the risks that really matter.

Emerging risk assessment should focus on plausibility and impact. Probability is notoriously challenging to assess for emerging risks and creating angst over this can act as a distraction. Formal assessments and heat maps should be exchanged for structured, creative discussions across business units and functions that bring different perspectives to bear on the topic and seek to strip away unhelpful biases. This will help organisations to better appreciate potential risk trajectories.

Scenarios are a good way of making emerging risks tangible, with a view to delineating or calculating the immediate and longer-term impacts on strategic, tactical and operational targets.

Airmic’s guide *Emerging risks: New world, new solutions*, released last year, further explains the importance of identifying, developing or leveraging the right basket of measures to mitigate key risks, noting that new risks can often be addressed by commonplace tools and fast action after the fact may be a more valid response for some risks than upfront actions.

Covid-19: Black swan or gray rhino?

Why have governments and businesses seemingly failed to prepare adequately for the coronavirus pandemic?

The pandemic cannot be referred as a “black swan”, as Nassim

Taleb has termed catastrophic events that are unpredictable. Pandemics have featured in the risk registers of many governments and organisations. It has been more of a “gray rhino”, as Michele Wucker would term it – a highly probable, high impact yet neglected threat – or else a “known unknown”, as the former US Secretary of Defense Donald Rumsfeld would have put it.

People today have no living memory of a pandemic like Covid-19. There has not been one on such a worldwide scale since the Spanish flu pandemic of 1918. For most organisations in the UK and Europe, pandemics dropped off their risk radars after the swine flu outbreak of 2009 to 2010. Some risk professionals believe there might have been some degree of complacency, but that was not the main issue.

In the World Economic Forum’s Global Risks Report 2020, pandemics were classified as a low probability, high impact risk. Even where the risk of pandemics was recognised, it was the geographic spread and the velocity of the Covid-19 pandemic that has taken many by surprise.

How risk professionals and their organisations responded

Most governments had been preparing extensively for pandemics. There have been a number of influenza pandemic simulation exercises in the UK over the years. Some organisations had also rehearsed their pandemic-related business continuity plans assiduously.

In last year’s Airmic survey, risk professionals were asked to imagine a “nightmare headline” they would dread reading about in the news. One of them feared a global travel ban because of a pandemic that hit the UK, long before the first cases of coronavirus infections were reported from the city of Wuhan.

But it was not so much the public health aspect of the pandemic that businesses were unprepared for. It was the debilitating economic impact of the lockdowns and national restrictions that many had not even contemplated.

Businesses have the risk of pandemics on their risk registers. One of our members reported anecdotally that for his organisation, which is involved in large-scale events, this risk had hovered around 20th place in its risk rankings. But that organisation’s response plans were focused on health and safety issues, and on public relations and communications. Generally, most organisations had prepared to respond to a localised disease, rather a global pandemic. It was even less likely that they had taken into account the near total ceasing of international travel, which would pose a direct hit to those in the hospitality industry, for instance.

Then there is the issue of the extent to which even large corporations can afford to prepare. Low-cost airlines, one of the major victims of the Covid-19 crisis, are generally prepared

to ground their entire fleet for up to a month if needed. Any scenario requiring a longer period of grounding had been seen as out of proportion for one organisation to deal with itself. Their business model of running on low margins does not accommodate the grounding of their fleet for an extensive period, which is exactly what the lockdowns and travel restrictions have wreaked.

Organisations with links in Asia, where the spread of Covid-19 started, may have reacted faster to the pandemic situation back in the UK and Europe than their counterparts without such interregional links. Major international events such as sporting events were very quickly cancelled around the world, after they were first cancelled across Asia. Even then, many organisations in the UK and Europe regarded the happenings as an 'educational piece' – useful to learn from, but not for any immediate application. That was partly because the advice of the authorities, such as the need to wear masks, had been conflicting. It reflected that the scientific evidence for the effectiveness of masks against the coronavirus had been inconclusive.

While there is a limit to which large corporations can afford to prepare for low probability, high impact events like the Covid-19 pandemic, the capacity for small and medium-sized enterprises (SMEs) to do likewise is even more constrained. The risks of SMEs have typically centred around cash flow issues in ordinary times. With the pandemic-related economic shutdown, their very survival as viable businesses is at stake.

Agility with effective leadership: The best response

Risk professionals have found that the most important principle in responding to the Covid-19 crisis is agility combined with effective leadership. For those in technically specialised industries, there is a tendency towards a kind of problem-solving mentality that emphasises meticulous attention to detail, especially crucial for highly regulated industries where health and safety issues are a non-negotiable. However, that can be frustratingly self-defeating for risk professionals if they have to deal with a large-scale crisis full of unknowns like the pandemic.

In such situations, it has been more important to be able to make good decisions and judgements as quickly as possible, so as not to be caught out by the next stage of surprises in an unfolding crisis. Excruciation over the details of action plans or the precise wording of statements should not come at the expense of an agile response.

These principles of crisis management response towards Covid-19 can also be applied to other types of crises.

The 'new normal': Risk management in the post-Covid-19 world

The Covid-19 situation is an opportunity for risk professionals to demonstrate the value of their work to their organisations.

They are having more contact with their senior management and are more firmly embedded in what their organisations are doing. This has resulted in the breaking down of barriers internally, and far more collaboration between functions in the organisation – all of which have taken place while risk professionals, like many other professionals, have been working remotely.

A pandemic demands integrated enterprise risk management – a set of practices and processes underpinned by culture and technology, geared towards improving decision-making and performance through an integrated view of how well an organisation manages its own set of risks.

Risk and security professionals play a vital part in ensuring the smooth and effective running of business. "Historically, their input has not been recognised to the degree it should have been," says Mike Hurst, Director of ASIS UK and of HJA Consult. "Organisations need to ensure that their risk and security teams are fully integrated into all areas. Enterprise Security Risk Management (ESRM), if properly applied, can help protect organisations and reduce the impact of adverse events and deliver a real return on investment."

At this time of writing, risk professionals are helping their organisations adapt to the new normal after the easing of Covid-19 lockdowns – defining what business-as-usual means for them and identifying the new risks involved. They are constantly reviewing their business continuity plans and taking the pulse of sector, national and international circumstances, which will continue to rapidly change.

"Clearly, the technology that enables people to work remotely has proved that it can meet the challenge of half the UK workforce working from home," says Sian Fisher, Chartered Insurance Institute (CII). "Any business that still has paper filing now knows what it has to do to adapt in future."

"One challenge we have is to help all our clients understand how they can adapt their businesses to a pandemic environment – giving them the kind of risk insights that they need and deserve."



An abstract graphic design on a dark blue background. It features several overlapping circles and arcs in various shades of blue and grey. A large, bold, white number '3' is the central focus, positioned in the lower-left quadrant. The circles and arcs create a sense of depth and movement, with some appearing as if they are behind or in front of others.

3

Nightmare headlines

Our survey respondents were asked to imagine a headline in the news they would dread reading most when they woke up in the morning.

Many responses naturally revolved around the coronavirus outbreak, which was in its early days in the UK and Europe. Soberingly, many worst-case scenarios in those imagined headlines relating to the coronavirus outbreak have almost all come true.

Using techniques such as imagining potential headlines to 'think the unthinkable' is helpful for identifying and assessing the emerging risks that do not typically make it into the risk registers of organisations.

Global travel ban as pandemic declared by WHO

London underground closes as coronavirus impact takes hold and funding runs out

Global carbon tariffs set to reduce air travel by 80% over next few years

Cyber-attacks on industrial systems bring industry to its knees

Brexit transition ends early – it's NO DEAL

Senior partner of firm implicated in serious fraud

ATM software failure leads to high street banking meltdown

Glass in baby milk leads to clearing of shelves and catastrophic product recall

Devastating multimillion fine imposed by Information Commissioner's Office for GDPR breach upheld by courts

Accusation of modern slavery hits high street chain, destroying its reputation overnight

4



Risks and megatrends

The average score on a scale of 1 to 5, where 1 means the megatrend is “not a concern”, and 5 means it is of a “very high concern”.

See Annex: Research & survey methodology, at the end of this report.



4A Cyber & technology

Written by Control Risks in collaboration with Airmic

The way we live now: how organisations can use technology to thrive in the post-Covid-19 world

If anyone doubted the importance of digital transformation to business, Covid-19 has underlined that reality with a vengeance.

Our new virtually enabled, data-driven and distributed homeworking has transformed the daily reality for millions of employees. It has also increased our vulnerability to cyber-attacks. Criminals have weaponised the fear and uncertainty of the pandemic to commit financial fraud and extort ransoms. Meanwhile state actors have focused on disruption, espionage and surveillance. The tactics are not new, but the scale and volume of the attacks have been. This has shone a stark light on those organisations that have not made significant progress in digitally transforming their operations.

Digital transformation is a nebulous term with many different definitions. At its heart, it is a way to empower an organisation with the skills, culture and data insights to enable innovation and growth. It is also a way to build resilience. Automation, Artificial Intelligence and cloud infrastructure, among other technological advancements, present huge opportunities. However, they also form the basis of a digital landscape that makes us more interconnected and thus more exposed than at any time before.

Our individual and corporate exposure to cyber threats is expanding at a rapid rate. Artificial Intelligence techniques, while still in their infancy, are being utilised in more state and criminal operations for faster and harder-to-detect attacks. Targeting of operational technology – the systems used to control industrial operations at manufacturing facilities, power plants and other critical infrastructure – is increasing as outdated analogue systems digitise and converge with IT networks at corporate headquarters.

Attacks in 2017 showed the prospect of global disruption Meanwhile, the targeting of cloud service providers and software supply chains continues to raise the spectre of cascading attacks that flow through the systems of global companies and their suppliers at unprecedented speed. We have already seen this in the contagion unleashed by several high-profile attacks in 2017. One of these, NotPetya, was

attributed by Western governments to Russia, causing billions of dollars in damage to public and private sector companies around the world.

The risk of getting caught up in such contagion is becoming ever more likely now that cyber-attacks have become a less covert and more conventional tool for states to project force. Unrestrained by international norms, the militarisation of cyberspace has quickened the commodification of attack tools now available to a wide range of threat actors, not just to national governments.

Just three years after NotPetya, organisations worldwide face the prospect of even bigger, faster and more impactful attacks. Already organisations face growing business interruption, response, recovery and remediation costs, as well as bigger cyber insurance premiums. Such challenges are especially relevant to companies that maintain and operate legacy systems now ill-suited to the digital age. The need for these companies to digitally transform is perhaps the most acute and is in the public interest, given many of them – some of the biggest organisations in the world – maintain sensitive data on all of us.

Diverging regulations complicate multinationals' strategies

Regulatory risk is also a growing challenge. As seamless global connectivity has grown in recent years, so conversely has the emergence of a fragmented regulatory backdrop. Whatever the debates over cause and effect, this has presented major compliance and operational headaches for international companies. As an example, China's Cyber Security Law, with its emphasis on data localisation and controls on cross-border data transfers, is forcing companies doing business in China to map their data flows and supply chain exposure, often with big implications for their operating models.

Where this differs from the EU's General Data Protection Regulation (GDPR) is in the notion of proportionality, which in Europe allows for exceptions based on criteria such as the data subject's consent and risk management. The underlying principle of GDPR and more recent legislation in California has been to shift the power balance from bulk data collection and surveillance to data privacy and consumer rights.



Trade tensions and 'sovereign internets' add to headaches

Politics only complicates this backdrop. Tensions between the US and China, and the rise of protectionism in the creation and trade of software and hardware, are catching global companies in the crossfire – just ask Huawei or Cisco. Companies are being required to weigh political and national security considerations when engaging with a supply chain partner about which their host government has a negative view.

Covid-19 will accelerate this underlying trend – an example is the decoupling of US and Chinese technology interdependence – with many companies seeking to move their production closer to their consumer base, especially in the pharmaceutical and medical services sectors. The growth of Internet controls in Russia, China and many African nations is raising the prospect of further fragmentation. The erecting of digital boundaries, a clear expression of a more assertive national self-interest, poses a threat to globally standardised electronic communications. Such boundaries could have a profound impact on the way we live and work.

The emergence of 'sovereign internets' cut off from the rest of the web is a clear test to the open vision with which the Internet was founded. However, some perspective is needed. Despite the challenges, the age of ubiquitous global connectivity is here to stay. The proliferation of Internet of Things (IoT) devices is such that they are predicted to overtake non-IoT connections in 2022. The computerisation of everything from cars to medical devices, homes, factories and cities is not going anywhere, a reality the Covid-19 pandemic has reinforced with the normalisation of our virtual homeworking set-ups. Likewise, digital transformation is at its core a way to build resilience against existential shocks, whether that is a pandemic, supply chain disruption or the day-to-day barrage of phishing and social engineering attacks.

How should organisations respond?

Fine-tuning risk management strategies to navigate the shifting political and regulatory tides and their impact on operating models is essential. Internal company functions will also need to adapt. In many larger international companies, we are already seeing a blending of physical and cyber security functions, merging once siloed structures to reflect the growth of attacks on systems whose disruption leads to a direct physical impact.

Organisations can prepare themselves for these emerging challenges in the coming years through further investment in highly automated security operations and intelligence centres – not least because mitigating risks and threats such as mass shootings, environmental activism, digital disruption and state-directed disinformation now requires active monitoring of online environments. Cyber-physical convergence is changing the world around us and focusing more light on the need for companies to recruit people with the skills to interpret the noise and chatter of these forums.

The critical success factor in any digital transformation programme is to ensure it is focused on people. Technology is a crucial catalyst in the process, but investment in skills and culture is a much more sustainable way of building a secure, compliant and resilient business in the information age. Promoting creativity will unlock the potential of global connectivity and the agility to navigate uncertain political, economic and regulatory headwinds.

Investment in people is also the only way to utilise the data insights that will increasingly shape strategic decision-making. These insights are the game changer and the key to making the most of a digital transformation programme.



4B

Climate & environment

As *The Economist* put it, “following the pandemic is like watching the climate crisis with your finger jammed on the fast-forward button”. The pandemic and the climate crisis have a number of similarities. They are no respecter of borders. They are low frequency/high impact catastrophic risks that do not tend to feature highly on the risk registers of most businesses.

It is widely thought that the Covid-19 lockdowns have restored clean air and brought emissions down, since economic activity has essentially ground to a halt. But the sobering finding is that even with such an unprecedented economic standstill, the world still has over 90% of the decarbonisation it needs to do to achieve the ultimate goal of keeping temperature rises to less than 1.5 degrees Celsius warmer than the average temperature before the Industrial Revolution.

While the Covid-19 crisis has occupied the full attention of governments, and rightly so, this has been to the detriment of urgent climate action. The latest Nationally Determined Contributions – pledges to cut emissions – submitted by a number of governments have shown no ratcheting up of their targets for cutting carbon emissions, which the Paris Agreement envisaged as necessary for keeping its goals for limiting increases in the global temperature. That includes governments that have otherwise been the vanguards of climate action. The 2020 United Nations Climate Change Conference slated to be held in November in Glasgow, also known as COP26, which would have provided the vital forum for governments to co-ordinate their climate action plans, has been postponed.

There is a real danger of kicking the can down the road. Businesses will bear the brunt of climate change, which is already posing risks to them today. Flooding and other extreme weather events have damaged assets and have disrupted business operations. These will cause knock-on effects that will disrupt supply chains and impact staff, ultimately leading to lost revenues and reputational damage, all of which will intensify over time.

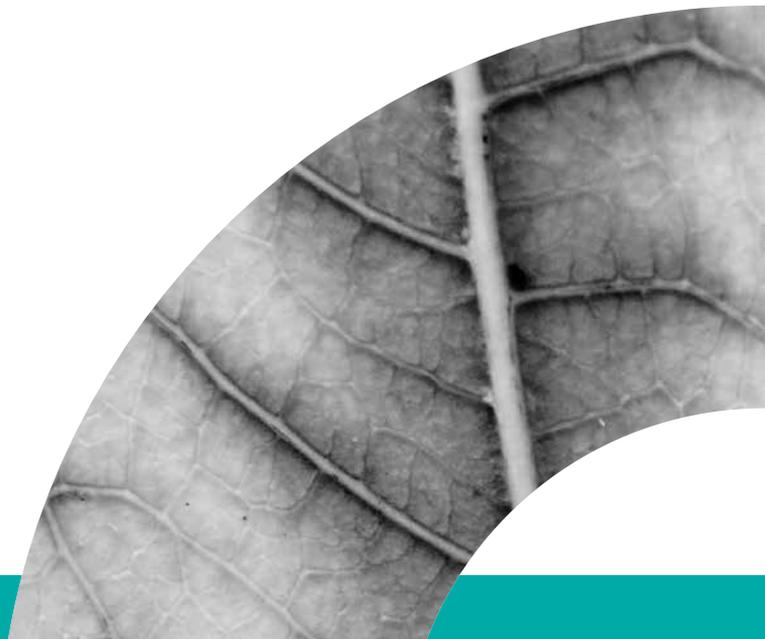
The perspectives of risk professionals and businesses

Yet, many businesses still see climate change as something for governments and NGOs to deal with and co-ordinate, and are unwilling to make investments towards that end. Most businesses are unlikely to take appropriate action unless forced to do so by legislation.

Boards in the private sector, focused on quarterly reporting and answering to their shareholders, are less driven by the urgency to tackle climate risks.

Such pressures leave companies with less bandwidth for complex environmental regulations and laws, which can be daunting to keep up with. Only 36.6% of our survey respondents felt informed with regard to legislative changes relating to climate change and environmental issues. Furthermore, 51% have not considered how their insurer will respond in the event of climate-related litigation or claims.

That said, the number of companies committing to net-zero





emissions by 2050 is increasing. Last year saw a slew of new commitments towards this end by some of the world's highest-emitting companies.

Climate-driven politics

With the intensifying nature of climate activism, from the Extinction Rebellion movement in the UK to the youth climate strikes catalysed by Greta Thunberg, climate issues are also shaping politics and ideology for a new generation. All this could transform the consumer sentiments of members of the next generation, who will increasingly shun fossil fuel-intensive industries, to which businesses must adjust.

It also goes beyond climate action. Climate-driven politics is one of the major forces behind the rise of 'millennial socialism', in which a response is enmeshed with a markedly leftist economic programme of massive public spending. The Green New Deal in the US, as championed by Democratic congresswoman Alexandria Ocasio-Cortez, calls for unprecedented levels of government borrowing to fund universal health care, a universal basic income and a jobs guarantee, as well as insisting on decarbonisation within a decade.

This in turn has implications for the future of climate policy, to which businesses ought to sit up and take notice. Instead of leaving it to the market, for example, through carbon taxes or carbon trading, such politics and ideology have a marked preference for central planning and regulation as the solution to climate change.

Climate change: The transition risks

If governments fail to mitigate climate risks with sufficient lead time, it will have the effect of increasing the transition risks. Businesses would be forced to adjust more rapidly, so as to achieve carbon budget goals when the climate situation gets more dire, leading to greater costs and disruptions.

There will also be widespread ramifications to society in the event of rapid adjustment to a low-carbon economy. Employees would have to retrain for new jobs more rapidly as old ones are displaced. When the price of carbon changes drastically within a short period of time, this will have knock-on effects on electricity tariffs, for example, which could have political consequences for governments.

There has been significant work in the policy area, such as the European Green deal, a set of policy proposals from the European Commission to make Europe climate neutral by 2050, as well as developments in the financial services sector such as the Task Force on Climate-related Financial Disclosures (TCFD) initiative, which seeks to develop voluntary, climate-related financial risk disclosures for use by companies in providing information to investors, lenders, insurers and other stakeholders.

"The extent to which green factors are incorporated into the Covid-19 recovery plans will be a major factor in determining the pace of transition to a low-carbon economy," says Dr Paul Pritchard, Senior Associate at Iken Associates, a sustainability consultancy. "Nonetheless, in the near term, I believe the material climate-related risks for many organisations will come from two directions.

"Firstly, potentially rapid shifts in market sentiment whereby certain products and services are deemed unacceptable, and secondly the increasing challenge coming from financial sector partners, as reflected in the TCFD initiative. The challenge from banks, insurers and investors will go beyond questions on carbon footprints to assess risks, and their financial implications, across their value chain, including suppliers."



4C

Trust & reputation

Written by KPMG in collaboration with Airmic

Trust and reputation have become increasingly important to businesses. According to AMO, the total value of global reputation last year was in excess of \$16 trillion. This has come at a time when social media carries the propensity for amplifying reputational damage, especially following activist events such as #MeToo.

With the Covid-19 pandemic, all businesses and organisations have been placed under additional stress. One might think they may be more easily forgiven for their errors, but consumers continue to find many corporate transgressions unacceptable.

A sports and fitness retailer in the UK received criticism for insisting on remaining open, despite non-essential businesses being ordered by the government to shut. At the same time, a pub chain faced a barrage of public criticism after saying it would stop paying staff wages until it had worked out details of the government furlough scheme.

Reputation: Capability versus character

One question that has perplexed many is why some companies and brands have suffered public criticism without any apparent impact on their success.

To better understand reputation, it is helpful to think of two types of reputation, as Rupert Younger and David Waller have laid out in their book *The Reputation Game*.

The first is the perception of an organisation's **capability**, or its products and services – a typically 'sticky' perception that is especially important for customers.

The second is the perception of an organisation's **character**, or the way it acts – this is typically very volatile and is especially important for counterparties who work with the organisation.

In 2015, an auto manufacturer admitted to using software to give false readings on exhaust emission levels in millions of its cars. However, its car sales were not impacted because of the company's 'capability reputation' for making great cars. Nevertheless, in the damage to its 'character reputation', the company had to pay €25 billion of counterparty costs relating to the scandal to regulators and investors, and its share price fell around 40% in a few days.

What drives reputation and trust?

Reputation has been defined as the "emotional connection between people and companies". The Airmic-Reputation Institute (now The RepTrak Company) guide *Defining and managing reputation risk: A framework for risk managers* identified seven core areas that drive an organisation's reputation and the trust that underpins it. These are: leadership, financial performance, products and services, innovation, workplace, governance and corporate citizenship.

Building a strong reputation requires delivering on these seven areas. If an organisation's stakeholders perceive it to be doing so, they will trust and support it. But this also goes the other way. If stakeholders do not see the organisation delivering on these seven areas, they will lose trust and not buy, recommend, invest in, work for or give it the benefit of the doubt.

In the Airmic survey this year, risk managers were most concerned about financial performance when it comes to what drives trust and reputation in their organisations, followed closely by issues of leadership and governance.

Intangible assets and reputation risks: Two principles for risk managers

In the Airmic-RepTrak guide, reputation is defined as the "emotional connection between stakeholders and organisation". Nevertheless, the growing importance placed by businesses and their customers on reputation comes in the context of the rising importance of intangible assets. According to MSCI, intangible assets represent as much as 80% of the value of S&P 500 companies, and even higher for companies in sectors such as IT and health care.

Traditional shareholder value, such as that pertaining to physical assets, is increasingly being replaced by broader stakeholder value. This means that organisations are required to manage broader critical trade-offs and critical risks, which makes the reputation risk landscape increasingly complex. Positive (or negative) reputation can have an influence on stock price, cost of doing business, customer churn, employee morale and leadership changes. There is some evidence that the stock price of organisations with high reputation scores tend to outperform the rest of the market, as research by The RepTrak Company shows.



Ranking	Driver
1	Financial performance
2	Leadership
3	Innovation
4	Governance
5	Products and services
6	Workplace
7	Corporate citizenship

The top drivers of reputation of concern to risk managers

There are two key principles that can allow risk managers to be more effective at addressing reputational perils. The first principle is proactivity. The most successful businesses undertake horizon-scanning regularly, to pick up any looming threats before they hit the organisation. Monitoring changing consumer sentiments or significant social movements outside their businesses can allow them to adjust before things potentially go terribly wrong.

Many businesses across industries manage reputational challenges in a reactive way, effectively becoming crisis managers. They constantly fight fires by launching PR campaigns, but often find that the damage has already been done.

The second principle is to find ways of working closely with risk owners. It could be a Chief Financial Officer, a Chief Marketing Officer, a Product Manager, a Communication Manager, or any other employee in charge of looking after reputation. We have seen many counterproductive cases of risk managers trying to minimise exposures without balancing them with the general business strategy and operational practices led by risk owners.

For example, when an oil and gas corporation decided to reposition itself as an environmentally responsible company through Corporate Social Responsibility, non-governmental organisations highlighted the contrast between the green content of its communications and the thrust of its core

business, which continued to be oil-focused. The situation was made worse after the corporation suffered an oil spill disaster.

Reputational risks: How can they be insured?

Even with great internal risk management in place, there might be aspects of reputational risks for which risk professionals may still want to seek insurance cover.

If reputational risks are to be insured, how can the value of an organisation's reputation be determined? That is a question that has preoccupied the industry for some time.

There has been progress made since the initial products from the early days, which focused on a pay-out mechanism intended mainly to cover the costs of crisis management, such as the costs of a counter-campaign conducted by a PR consultancy. There are now more sophisticated insurance covers which incorporate data analytics to measure a more comprehensive range of damage from a negative event and even the real-time monitoring of developing crises.

A robust framework is needed for measuring reputational damage and its related costs to an organisation, which must satisfy all parties. Real-time measurement and alerting are also becoming vital for companies to ward off potential risks to their reputation.

Loss of trust in information sources, governments and elites

The 2020 Edelman Trust Barometer found that business ranks highest in competence, holding a massive 54-point edge over government as an institution that is good at what it does (64% compared to 10%). But there are two different trust realities. The informed public – wealthier, more educated and frequent consumers of news – remain far more trusting of government, business, NGOs and media than the mass population. This has been driven by a deepening sense of inequity and unfairness in the system, where the perception is that institutions increasingly serve the interests of the few rather than the many.

According to the Airmic survey, risk managers are less concerned about the trends surrounding the loss of trust in information sources and in governments, compared to the reputational risks to their companies around regulatory failings and social media-driven risks like the #MeToo allegations.

But risk managers should not underestimate how the phenomenon of fake news and disinformation campaigns can impact their businesses and organisations in very direct ways. During the Covid-19 pandemic, conspiracy theories gained traction in online circles that it was 5G telecoms equipment that was causing coronavirus infections, even though scientists have repeatedly said that it is scientifically impossible for any connection between 5G and Covid-19, a disease spread by respiratory droplets. Consequently, multiple telecoms masts across the UK and Europe were set on fire and destroyed, and even telecoms employees not deployed to work on 5G installations at all have been physically attacked.

Even large corporations may feel that fighting the war on disinformation is beyond their remit and means. But organisations should at least proactively monitor fake news stories, especially where it concerns their sector. They should address those stories swiftly, with detailed and causal explanations, rather than merely issuing statements to refute false claims when it is too late.



4D Geopolitics & populism

Written by Willis Towers Watson in collaboration with Airmic

"A week is a long time in politics," UK prime minister Harold Wilson supposedly said. Given the pace of geopolitical change since the pandemic lockdowns began, Wilson's remark has at times seemed an understatement.

Unsurprisingly, then, there have been dramatic shifts in the relative position amongst the megatrends relating to geopolitics and populism since last year's survey.

'Political uncertainty' as a general concern has fallen to tenth place, from third place last year. The related risk megatrends of societal change/unrest, generalised trade disputes, outbreak of war and tech wars now feature lower on the list of 25 megatrends.

On the other hand, 'regulatory uncertainties (e.g. Brexit)' has risen to fifth position. Evidently, fears of general political uncertainties and trade wars have been replaced by a specific concern for many UK companies, as the UK heads into final negotiations with the European Union.

Moreover, the 'global economic outlook' as a geopolitical risk megatrend is now the third-highest ranked megatrend, up from last year, as Covid-19 has delivered a devastating economic shock to many countries.

The nature of risks today – especially geopolitical risks – is that they are increasingly interconnected. Geopolitical threats manifest in a wide variety of ways, which are often unpredictable. For instance, cyber risks, which rank at the top of the megatrends table this year, often contain a significant geopolitical element.

Indeed, while much has changed, there is a surprising element of continuity in the geopolitical threats that companies face in the Covid-19 era.

The era of Covid-19: greater uncertainties and tensions

While the Covid-19 pandemic is primarily a problem of human health, it has carried inevitable consequences for geopolitics as well as domestic politics. After all, geopolitics is about how businesses sit within the economy, policy and geography, and the impact that events such as pandemics have on this relationship.

Trade disputes

The global pandemic could have served as a chance for more co-operation between the US and China, as some mused early on. Instead, analysts are now warning of a new Cold War between the two powers. The on-off trade disputes between the US and China, which created uncertainty for the global economy in the last few years, look likely to continue unabated.

There are also new trade issues occasioned by the COVID-19 crisis. For instance, governments around the world have banned the export of health care equipment and medicines, disrupting the global supply chains that matter most in the crisis.

Tech wars

Aside from Brexit, perhaps the world's most dramatic trade negotiations have been related to the so-called 'tech war' between the US and China. Thus far, headline issues in the tech war have centred around the concerns of the US administration regarding the Chinese telecoms giant Huawei. This has led to other countries finding themselves in a delicate position between the US and China.

As of this time of writing, US-China tensions in this area are continuing to escalate, despite progress in 'phase one' trade talks.

Cyber risks

As employees began to work from home in compliance with the lockdowns around the world, this exposed their organisations to increased cyber risks and breaches – because data normally accessed in the secured office environment is



now taken into homes. Organisations need to improve their cyber and business resilience to continue to operate in this way and maintain their reputations.

Economic outlook

A debt crisis among emerging markets is growing as developing countries face a wave of government bankruptcies, due to the global economy going into shutdown. More than 100 countries have sought financial assistance from the International Monetary Fund, including large emerging markets such as South Africa.

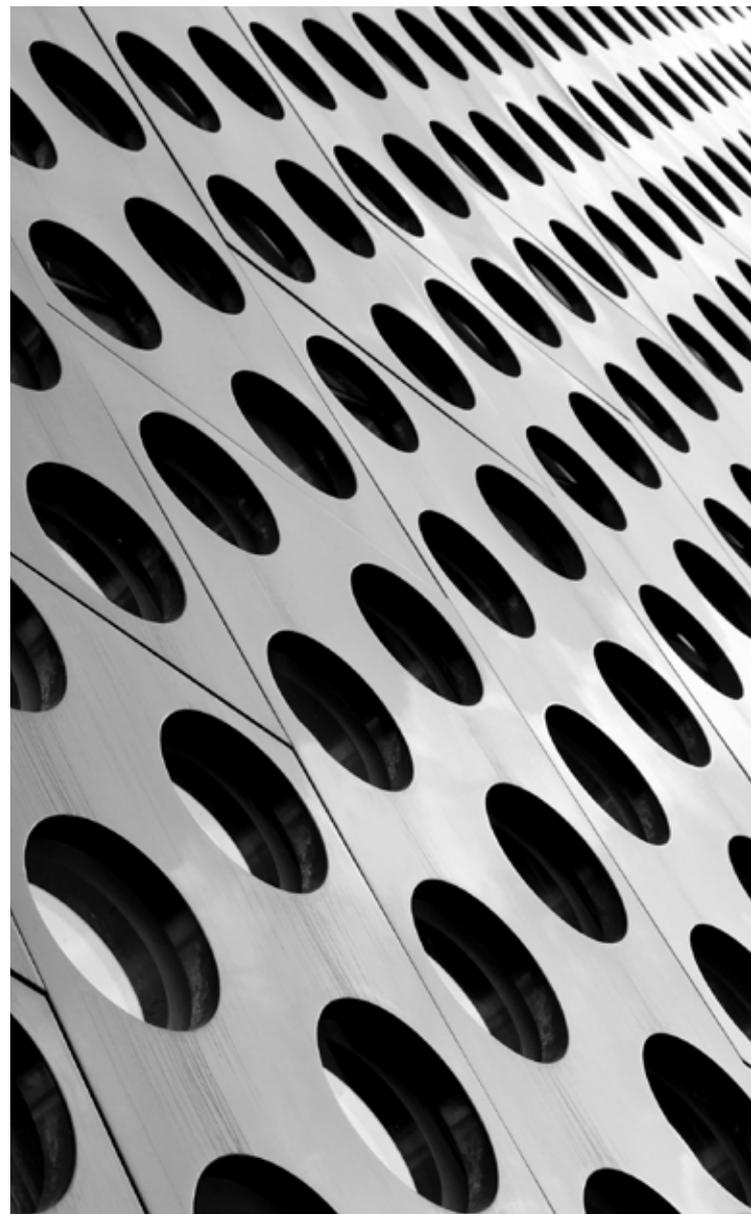
Populism

The Covid-19 pandemic threatens to spark a new wave of Euroscepticism and populist politics. For instance, in Italy, the first epicentre of the pandemic in Europe, a poll found that 88% of its people felt the EU had failed them – which could provide fertile ground for anti-Europe campaigns.

Climate action

Many have remarked on the diminished pollution associated with the pandemic's disruption of industrial activity. Despite calls by many for a green recovery from the coronavirus crisis, there is also a risk that local and global efforts to tackle climate change are flagging, as other risks seem to be taking priority. The postponement of the 2020 United Nations Climate Change Conference (COP26) to be held in Glasgow is also reducing the pressure on governments.

Yet, proactive climate action will put organisations at a competitive advantage given that all listed companies and large asset owners in the UK are expected to make disclosures using the Task Force Climate-related Financial Disclosures guidelines by 2022. The pandemic crisis has also shown that an organisation's corporate brand is very important for its performance and a clear climate agenda is increasingly a lever for corporate reputation. The post-Covid-19 world offers a great opportunity for employers to redesign or accelerate the future of work, with less travel and more remote working and use of technology, which may well



improve their green credentials.

Understanding the connectivity of geopolitical risks

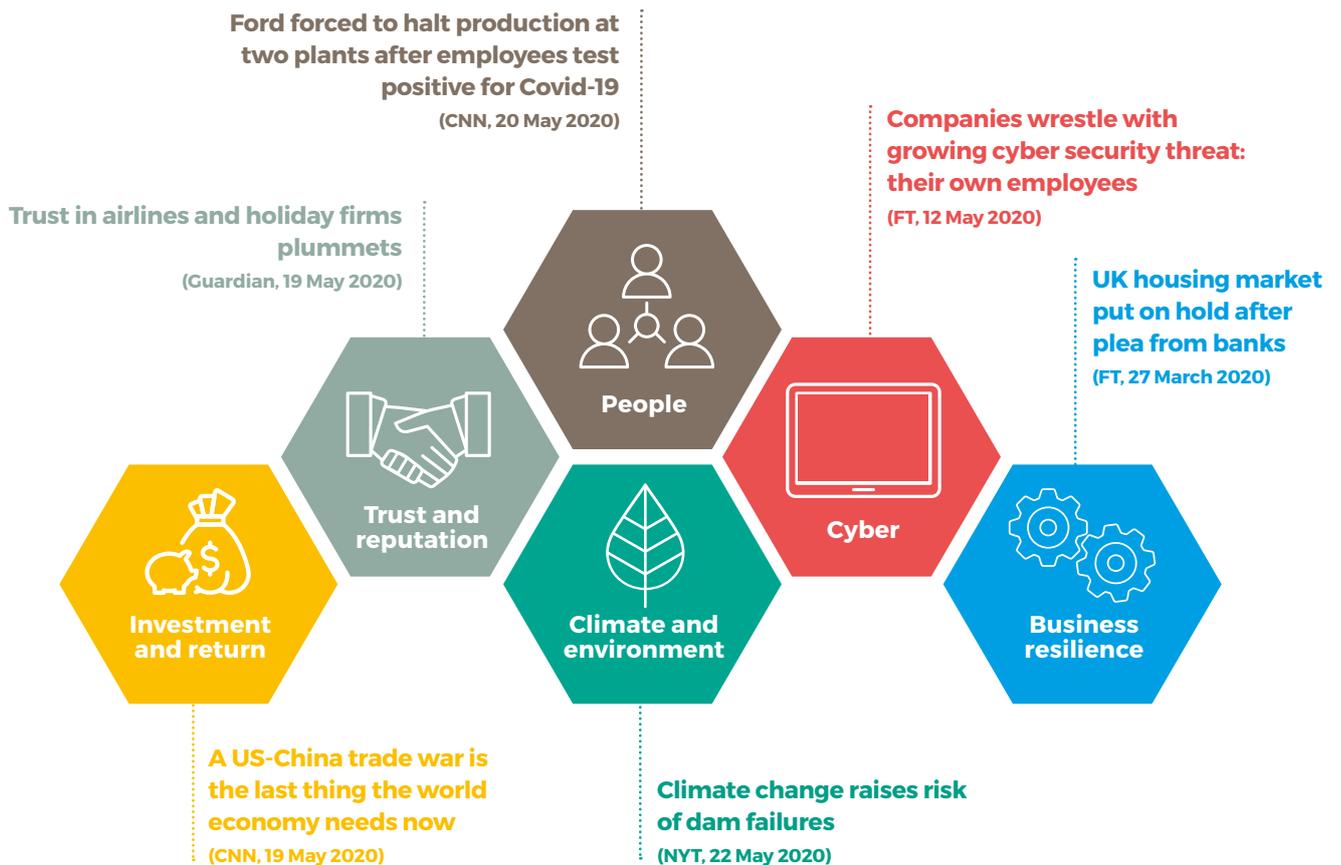
Geopolitical threats manifest in a wide variety of ways, which are often unpredictable. To tackle geopolitical and political risks, organisations must first identify their exposures to a landscape that is fast-evolving, interconnected and complex.

These threats not only affect multinational companies, which are naturally confronted with a long list of risks, but also small and medium-sized enterprises which are also exposed to changes in regulations and trading relationships. For example, if a production site is hit by a sudden export ban, as has frequently been the case during the Covid-19 crisis, it needs to

be agile and able to move production and people, or to contain costs while the site is out of action.

Analysing the geopolitical risks through ‘six lenses’ and their drivers is a framework approach that will help organisations begin to understand their exposure from a 360° perspective and the interconnected nature of the challenge in front of them.

Once an organisation identifies, understands and prioritises the risks it faces, it should be better prepared with response plans, including contingency and crisis management plans. Interconnected risks require integrated solutions that must be tailored and address insurable and non-insurable risks seamlessly.



Responding to a geopolitical event will usually focus on risks to people, assets, revenue and reputation. However, risks to business and value chain resilience, the climate and the environment, and cyber risks should be added to the list due to the interconnected nature of the risks.



Key stages of action: The three phases of action for organisations and their leaders in responding to the Covid-19 pandemic

The key here is advance planning, so that maximum attention and resources can be dedicated to action once a crisis hits – precisely at a time when both attention and resources are in short supply.

Operating in the post-crisis new normal

With Covid-19 continuing to unfold across the world – and countries at different points in their infection curves – organisations and risk professionals should give particular thought to how they will operate through the crisis if they don't have advanced planning to lean on.

If organisations can pre-empt the changes in the way businesses and the economy will operate in the ensuing six to 12 months, they can move from reacting into strategic planning that will help them to gain competitive advantage in the new normal and stay resilient. This is essential because all the other risks won't go away – cyber-attacks, floods, earthquakes and terrorism incidents could all still occur.

Breaking down activities into these steps as part of a roadmap will help bring focus and unity of action, and allow businesses to align to government decision-making and be

ready to operate in the new world.

Each of these stages is a new environment, so go back to basics and:

- Understand the new environment through relevant intelligence, assessment and quantification to comprehend the interlinked drivers and impacts on a business.
- Identify and assess. Ensure you are employing all the tools available to collate and interpret the information and then deploy subjective and objective assessment to inform the organisation's integrated decision-making.
- Prevent and protect. As the geopolitical landscape changes, so must the way in which risk leaders protect their businesses. A thorough understanding of the interlinked geopolitical risk drivers and their impacts provides a strong foundation for prevention and protection against them.

Remember that it isn't all negatives, the Covid-19 experience may bring opportunities such as the opportunity to evaluate different and more cost-effective ways of working, build a more resilient society, develop larger domestic markets and establish more reliable supply chains.

Either way, boards need to be ready and able to seize the moment and adjust their course appropriately. Risk professionals are in the perfect position to help them get there.

4E Governance, laws & regulation

Written by AIG in collaboration with Airmic

Organisations face extremely turbulent times, both economically and geopolitically. As we can see from the findings of this Airmic survey, risks in relation to governance, laws and regulation continue to raise a significant level of concern for risk professionals and their organisations.

Digital focus increases

Compliance with evolving digital regulations continues to be among the top risks of concern to risk professionals over the medium term, and ties in with the overall importance of the cyber and technology megatrend. Data protection and privacy have been areas of high concern for boards for a while now, with recently introduced General Data Protection Regulation (GDPR) already resulting in public fines which in severe cases could reach up to the greater of €20 million or 4% of worldwide annual revenue. The upcoming duty of care laws to protect children from online harms, when introduced, will add to this area of focus. Good cyber security governance is essential in reducing potential D&O liability. AIG supports the educational initiatives of the Internet Security Alliance (ISA) in producing cyber security practical handbooks and toolkits for boards in the UK¹ and, most recently, Europe.²

D&O liability – perceptions versus reality

We see through our D&O claims notifications that scrutiny of the decisions made by directors and officers is intensifying. But one of the interesting findings in the survey is that heightening shareholder litigation risk was of lesser concern to respondents than their corporate governance and regulatory

related exposures. This is surprising in today's economic environment and shines a light on the differences in individual perceptions versus the reality of D&O liability risk for even the best managers of the best-run companies ("it couldn't happen to us"). More and more corporate boards are being forced to defend themselves and their companies from a growing range of allegations involving matters such as bribery, corruption, sanctions, regulatory breaches and cyber security. New issues and exposures have also recently emerged, informed by movements such as #MeToo.

At the time of writing, due to unprecedented changes in business practices, including the implementation of business continuity plans and supply chain stresses, new or previously untested vulnerabilities may come to light.

It is insolvency risk – which is one of the most fundamental reasons why companies buy D&O insurance – that is perhaps most likely to confront many companies as the 2020 global economic downturn deepens. It is noted that worsening economic outlook is the third-highest risk concern across all categories surveyed, and that concern will likely have only increased since the pandemic began.

Core regulatory issues, bribery and corruption, and sanctions ever present

Currently, Brexit-related regulatory uncertainties persist as both parties to the withdrawal agreement have still to reach an agreement on several aspects of their relationship after the

€20 million

The General Data Protection Regulation (GDPR) is already resulting in public fines which in severe cases could reach up to the greater of €20 million or 4% of worldwide annual revenue



period of transition. The current environment is likely to add even more uncertainty to the negotiation process itself and has averted focus from the ongoing need for ultimate resolution of Brexit.

The current environment also may distract from risks relating to sanctions, regulatory activity, trade tariffs, bribery, corruption and anti-money laundering, but these risks continue to have material implications for boards and risk professionals. These risks are ever expanding, as evidenced by increased US pressure on Iran and the burgeoning trade war between the US and China over technology equipment and possible security threats.

In the UK, a new sanctions regime created by the Sanctions and Anti-Money Laundering Act 2018 (the Sanctions Act) will supersede EU sanctions on 31 December 2020, when the transition period of the UK's withdrawal from the EU ends.

Enacted so that the UK can continue upholding its international obligations following withdrawal from the EU, the act will give the UK government wider powers to implement sanctions, including financial sanctions, trade sanctions and immigration sanctions.

Companies doing business in the UK would thus need to adjust their sanctions compliance practices. They would need to familiarise themselves with these changes and the further regulations that are expected to follow, including seeking advice from external counsel.

What can risk professionals do?

Businesses and their boards that are informed enough to anticipate threats, prepare for them, stress test and adapt accordingly will be best placed to persevere in this climate. What this requires is strong corporate governance and robust enterprise risk management that gives organisations room to innovate while managing the risks of their ongoing business. Corporate directors and officers who are attuned to their organisation's risk profile, tolerance and response will also have a greater appreciation and understanding of the exposure of their own personal liabilities. This is where D&O insurance is

a key component of a company's risk management strategy, which will enable, as well as protect, directors and officers.

Organisations and risk professionals should read and understand the impact of the Financial Reporting Council's (FRC) latest UK Corporate Governance Code, which came into effect on 1 January 2019. This revised code places greater emphasis on the alignment and monitoring of corporate culture, as well as diversity and inclusion. These provisions reflect the changing risk landscape for the senior leaders of organisations, which at present is extraordinary in scope.

While activity from regulators and enforcement agencies is increasing, the cost of legal defence is also rising but at an alarming rate. Consequently, risk and insurance professionals should consider how they can contribute to and lead efforts to mitigate these risks for their organisations. That strategy should include not just purchasing sufficient levels of D&O insurance, but making effective use of it so that it becomes an invaluable tool to protect directors and officers. Working with an experienced D&O insurer and broker can also provide expert guidance regarding the claims process, insights on common claims to help reduce the personal exposure of individuals, tactics to contain costs and access to specialist knowledge when required.

"Corporate risk professionals need to have an acute understanding of the types of D&O products they buy, the carriers they buy them from, how much they buy and, ultimately, how they expect that insurance to respond in the event of a claim. All too often these decisions are reflected upon in times of crisis in situations where time is of the essence, instead of at point of purchase," says Christopher Magee, Head of Commercial D&O at AIG. "The directors whom the policy covers should be fully involved in the risk strategy and risk management process of the organisation. Sense checking and stress testing of certain high-risk exposures can also help ERM professionals and their boards identify any potential coverage gaps and obstacles that could arise in an actual claims scenario."

The guide to D&O insurance produced jointly by Airmic and AIG in 2018 provides further information and advice.³

¹ <https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/cyber-risk-directors-handbook.pdf>

² https://www.aig.lu/en/ferma-insights-2019/cyber-risks-oversight?cmpid=SMC-tw-AIGemea-EMEA_EcoDa-20200508082700

³ <https://www.airmic.com/technical/library/directors-officers-liability>

RESILIENCE IN AN
UNPREDICTABLE YEAR

A large, stylized number '5' is the central focus of the page. It is composed of several overlapping, semi-transparent circular and arc-like shapes in various shades of blue and grey, creating a layered, geometric effect. The number is positioned in the lower-left quadrant of the page.

5

Resilience in an unpredictable year

Written by QBE in collaboration with Airmic

Even before 'coronavirus' became the dreaded catchword around the world, the writing was already on the wall – 2020 was set to be a year of heightened unpredictability.

The UK general election of December 2019 might have settled the Brexit question, but uncertainty over the post-transition arrangement between the UK and the EU remains, with the risk of a no-deal scenario still a possibility. Meanwhile in the US, voters will decide whether President Donald Trump will win another term in office, while its trade wars with China and the EU will continue to hamper global trade and economic growth.

The Covid-19 pandemic has brought uncertainty to a whole new level. While there is much debate as to whether governments and businesses could have been better prepared for the outbreak of Covid-19, it has had the effect of exacerbating trade-related risks, people risks and cyber risks.

As the UK moved into lockdown in March 2020, our survey respondents were most concerned about business interruption following a cyber event in terms of the principal risks they face today, the loss of reputation and brand value, and the failure of operational resilience, while diseases and pandemics was placed just fourth on the list.

While the coronavirus outbreak is the overriding preoccupation of risk managers today, what the findings point to is that the Covid-19 crisis is manifesting itself through the megatrends and medium-term risks such as trade-related risks, people risks and cyber risks.

Unpredictability

Published in 2019, the QBE Unpredictability Index tracked a set of indicators between 1987 to 2017 across five pillars – business, economic, environmental, political and societal – to determine whether the world was becoming more unpredictable. The research also surveyed 1,300 business leaders from across the UK, France, Spain, Germany, Italy and the Nordic countries to examine how prepared businesses felt they were for the future.

According to the Index, the world is a less predictable place for businesses. Almost all of the 'least predictable years' in the Index have occurred in the past 20 years, with the majority during the past ten years. Interestingly, the research also showed that periods of unpredictability come in five-year cycles and the next peak was expected to hit in 2020.

"Our research suggests that periods of instability are getting longer and that we are perhaps seeing a trend emerge," says Cécile Fresneau, UK Executive Director at QBE. "The most unpredictable years in our index were 2010 and 2015, and already last year, we were predicting 2020 to be another year of heightened unpredictability."

Periods of unpredictability seem to be cyclical because of the nature of macroeconomic measures and electoral cycles. Nevertheless, the implications of growing unpredictability for business are many and varied, and can be felt and indeed driven by the megatrends discussed in this report. Unpredictability could lead to more volatile earnings, given uncertain demand and potentially higher costs. Climate change is already exposing assets and supply chains to more intense storms, floods and rising sea levels. Just

as the business operating environment is becoming more complex, regulations, governance and reporting requirements are increasing. Businesses and their senior managers are being held more accountable for their actions, evidenced by increased litigation and regulatory scrutiny for companies and their directors. Stakeholder expectations of corporate behaviour and ethics are also changing.

“One of the most striking findings of our research was the interconnectedness of factors,” says Cécile Fresneau. “Volatility in one area can have repercussions in another, prolonging a period of uncertainty and exacerbating its affect. With this in mind, businesses must consider the megatrends outlined in this report in terms of how they interact and agitate one other, and develop resilience plans that address the entirety of the risk and the reality of its impact.”

The QBE Unpredictability Index findings strike a chord with the Airmic member research, which shows increasing concern among risk managers for political and social developments, as well as broader technological changes and climate change.

Resilience

One of the most concerning findings of the QBE Unpredictability research was the level of optimism among businesses about their ability to deal with unforeseen events, compared to the steps they were taking to mitigate the risks. Three in four businesses QBE spoke to felt positive about their ability to deal with unpredictable events, but only 29% had risk management plans in place for such events, while even less (17%) carried out stress tests.

The Airmic Resilience and Transformation Model, introduced in the 2018 publication *Roads to Revolution*, lays out eight principles for achieving resilience in the digital age.

They include the proactive principles seen in resilient organisations that operate an exceptional risk radar focused on emerging risks, as well as the reactive principles seen in resilient organisations that review and adapt to changes and adverse events.

Furthermore, transformational organisations additionally require specific focus on protection and enhancement of the reputation of the organisation. This can often result in more successful crisis management, which is pertinent in this time of the Covid-19 pandemic. When successfully achieved, it can build the reputation of the organisation by

demonstrating the quality of management and governance capabilities within the organisation.

“Businesses and their leaders will not be able to rely on the defences of the past to manage the risks of the future,” says Cécile Fresneau. “They will need to develop new skills and tools to identify, understand and mitigate risk, and they will need to be open to collaboration. Many of the emerging challenges – such as mitigating the effects of climate change or protecting complex digital supply chains – will require organisations to work in partnership and build collective resilience.”

Conclusion

Preparing for risks on the scale of the Covid-19 pandemic may well be a task beyond the capacity of businesses and even some governments. Pandemics often feature as high impact but nevertheless low likelihood events in the risk registers of companies, which mitigates against boards and executives dedicating ever more resource to pandemic preparedness.

That is where businesses and organisations can take a leaf out of QBE’s Unpredictability Index. If waves of unpredictability indeed continue to occur in five-year cycles, it provides a timeframe for them to map out their risk horizon and consequently their investments into measures to control those risks and megatrends.

“Risk management is part of the antidote to unpredictability, but some threats are more existential,” says Cécile Fresneau. “Adaptation is critical to surviving and thriving in uncertain times. Business strategies and operating models need to reflect changing environments and investments made – in terms of both time and money – to ensure companies have the wherewithal to deal with the risks of today and tomorrow.

“As the size and complexity of risk grows, risk management and governance frameworks are becoming more sophisticated, and boards are increasingly demanding better information on risk. Challenging questions need to be asked about the sustainability of a business and its continued relevance to its customers. Equally, boards need to fully understand their worst-case scenarios and be confident that, balance sheet constraints notwithstanding, the steps taken to manage these risks are enough. Unpredictability is also a tremendous source of upside risk, as it provides opportunities for those who are willing and able to be more creative and bold to thrive with new services, products and business models.”

Preparation is the key to building resilience. Organisations that survive and succeed in an environment of enhanced unpredictability will be those that are best prepared.



6



Insurance faces a seismic shift

The insurance buyers: A profile

Airmic members are important insurance buyers. The estimated total annual insurance spend for the organisations that Airmic members represent is £10.5 billion. Additionally, they spend an annual total of £75.8 million on professional fees for risk management services and £254.2 million for insurance services such as broker's fees.

The harsh market: Declining affordability, narrowing options

Directors and officers liability, cyber-attack, supply chain failure and reputation risks have regularly featured among the top principal risks that Airmic members seek to insure. Increasingly, they say that the lack of adequate cover at an affordable premium is emerging as a risk in itself.

A survey conducted by Airmic in January 2020 found that rates have risen for almost all businesses. The impact of the hardening market goes beyond price, with reduced capacity, an increase in exclusions and unavailability of cover for some having a significant impact on 2019 renewals.

D&O rates have been hardest hit, with over 80% of respondents noting price rises in the UK. Of these respondents, 13% have seen D&O rates more than double.

There is frustration at poor or late communication from insurance partners, and over half of policyholders are only partially satisfied or not satisfied with the service from brokers.

The majority of businesses are exploring alternative risk transfer solutions, including new and greater use of captives, for their 2020 renewals. Over a third of respondents plan to invest more in risk management solutions.

In the lead-up to the current hard market, the sentiment among insurance buyers was that the market has offered them fewer options over the past decade. But businesses today are so complex, with each so different from the other, as to preclude the usefulness of one-size-fits-all products.

One large company reminisced how insurance tended to provide more value during the height of the soft market 15 years ago, while as much as 75% of their risks today could be uninsured. Meanwhile, SMEs feel forced to buy common all-encompassing policies such as Property Damage & Business Interruption (PDBI) insurance, whereas what they really need is cover for business interruption rather than for damage to their stocks.

"Today's market conditions are notably different to previous hard markets, which were cyclical and focused on price," says Julia Graham, Deputy CEO and Technical Director at Airmic. "Today, by comparison, we are also seeing reduced capacity, an increase in exclusions and, in some cases, the complete withdrawal of cover. There are also early signs of changing claims behaviour, which we are monitoring closely. This is a seismic shift.

"To stay relevant, the market must become more customer-centric, make better use of technology to improve service and provide more innovative solutions."

Enter Covid-19

Understandably, companies' frustrations have come to a head as those all-risks policies they thought they had bought did not perform as expected, and they started experiencing delays and rejections on claims they had filed in relation to Covid-19 disruptions. They often face a lack of clarity as to whether their policies even cover those situations.

£10.5 billion

The estimated total annual insurance spend for the organisations that Airmic members represent

Some Airmic members report that the pandemic has been regarded as an event their insurers did not intend to cover in their policies. Others have been engaged with their insurers on technical questions such as defining when and where the pandemic started, and whether it is to be considered one international event or many localised ones.

This has led to growing concerns over the renewal of their policies, if they had not already seen mid-term exclusions enacted. Those who have not previously bought captive insurance are now starting to consider that alternative to their traditional insurer.

That said, insurance buyers acknowledge that not all the challenges they face can be pinned on their insurers and brokers. Boards and senior managements have typically viewed insurance as a grudge purchase, for which no more should be spent than is necessary. The result often is that the policy they end up with is not fit for purpose. In the market, this has created a race to the bottom, at least on the depth and breadth of policy coverage.

Going forward, insurance buyers will certainly use the Covid-19 crisis to press home the importance of insurance to their boards and senior management. But insurance buyers are also in a mood for more far-reaching action, such as calling for networks of insurance buyers to be set up to apply pressure on the market to go back to standalone covers.

Working together: insurers, brokers and the buyers

“The insurance industry is at the crossroads,” says John Ludlow, CEO of Airmic. “Our member surveys suggest the hardening market is already forcing businesses to look at alternative transfer options, and an ill-judged response to the pandemic could detonate the whole mix.”

Following consultation with members, Airmic has called for last-minute and poorly communicated changes to be avoided in underwriting policy, including cover limits and exclusions, as well as constructive dialogue in wording disputes and a willingness to look favourably on grey area claims. Airmic has also called for flexibility in cover and rebates for reduced risk exposure relevant to current trading conditions and business operations, and for a recognition of the cumulative impact of the harsh market and pandemic on renewals.

“Covid-19 has had an unprecedented impact on the industry,” says James Dalton, Director of General Insurance Policy at the Association of British Insurers (ABI). “From shifting day-to-day operations to remote working, providing extra support and help to customers, to dealing with valid Covid-19 claims as quickly and efficiently as possible, no one in the industry has experienced anything like this ever before.

“While it is a fact that few firms will have bought the cover to enable them to claim for Covid-19 losses, for those that have, insurers have been paying claims as quickly as possible, including making interim payments.

“This will be a significant insured event – ABI members alone expect to pay around £1.2 billion, including £900 million in business interruption claims and a record £275 million in travel insurance claims. The total insured bill could be around £1.7 billion including claims paid by Lloyd’s.”

On 18 May 2020, the UK’s Financial Conduct Authority introduced a series of temporary measures to help customers holding insurance and premium finance products and who are in financial difficulty because of the Covid-19 situation. The measures include premium reductions, discounts, waiving fees and payment deferrals.

While insurers and brokers are under stress themselves, they have indicated they want to be business partners with Airmic members.



The insurance industry is at the crossroads. Our member surveys suggest the hardening market is already forcing businesses to look at alternative transfer options, and an ill-judged response to the pandemic could detonate the whole mix.

John Ludlow, CEO of Airmic

“Covid-19 has and continues to impact every aspect of our society,” says Steve White, Chief Executive of the British Insurance Brokers’ Association (BIBA). “Of course, the insurance sector has been central to some of these impacts, with billions of pounds paid in claims. BIBA member brokers are working to reassure their clients, to help them get the cover they need and to advocate for them where they have a valid claim.

“This sector, like others, has adapted to different ways of working and increased collaboration. A positive that I expect to see is the commitment to greater transparency for customers, to policy wordings that are easier to understand – a commitment in our 2020 Manifesto – and more certainty for policyholders.”

It is indeed in the interests of all parties to work together openly and constructively, particularly at this time of the Covid-19 crisis.

“With the vast majority of commercial insurance purchased through an intermediary, this crisis has highlighted how vital it for advisers to ensure that their clients understand the policy they are proposing to purchase and that they have the cover they need,” says James Dalton of ABI. “For insurers, the onus will continue to be on ensuring that policy wordings are as clear as possible.

“All sectors of the industry need to work together to learn the lessons that result from this crisis. Crucial to that will be rebuilding confidence and trust among businesses, reinforcing to society the vital role that insurance plays in supporting and protecting people against the day-to-day risks that they face. No country in the world can offer widespread pandemic insurance without government support, and we will need a conversation as an industry and as a society about how best to make insurance cover for pandemics more widely available and affordable.”

On insurance professionals, Sian Fisher, CEO of the Chartered Insurance Institute, says: “One area where we think that the profession as a whole can adapt is to look at the ‘whole customer’. For example, when we give advice to customers, it shouldn’t just be transactional advice about a series of products. It should look at all the customer’s risks – both insurable and uninsurable – and it should set out the best ways to mitigate against those risks.”

Airmic is working with industry, regulators and government bodies to explore how to turn this into a reality. Looking beyond the pandemic too, Airmic supports the creation of national catastrophic pooling and reinsurance mechanisms, such as the existing UK pools for terrorism and flood.

Trade credit risk, where customers could become bankrupt before paying for the goods they have ordered, is also among a growing host of issues impacting businesses as a result of the pandemic. On 13 May 2020, the UK government announced it would step in to guarantee trade credit insurance to ensure that the market does not seize up.

Nevertheless, Airmic believes these pools would have to be embedded in broader national and international risk strategies and should themselves be pooled to ensure the efficient use of capital.

Insurtech and innovation

At crunch times, innovation in the industry is needed more than ever to see all parties through the additional challenges. Fifty-seven percent of our survey respondents believe that the insurance industry is embracing innovation and insurtech, but that more could be done.

While the insurtech space is growing and has been attracting a significant amount of capital from the venture capital market, Airmic members have shared anecdotal instances of how it still takes months to obtain an insurance invoice at times. To them, this suggests an uneven level of innovation in the insurance landscape. Airmic members emphasise how the industry needs to demonstrate greater efficiency, as well as the importance it places on the basics of insurance risk transfer.

That said, the recent Covid-19 lockdowns have provided a jolt to the industry as a whole to move more quickly with digital transformation. There may indeed be a silver lining to every crisis, and many hope the pandemic will spur the industry on to greater efficiency through digitisation.





In responding to the Covid-19 crisis, agility combined with effective leadership is among the most important traits for risk professionals.

Conclusion

Risk professionals are operating in a world of volatility, uncertainty, complexity and ambiguity. The Covid-19 crisis has brought that to a whole new level, putting the profession to the test.

The key is velocity. The pandemic is a classic example of a low probability, high impact risk that has been exacerbated by the speed at which it has spread around the world. Much of this is due to the interconnectedness of risks in the era of globalisation.

As Airmic's *Roads to Revolution* report pointed out, because the underlying business and organisational dynamics today are so different from those of the past, they trigger the need for a major rewiring of both risk management and governance. For instance, the digital revolution should not be dealt with just as a cyber security issue, important as that is for any organisation. Boards will have to reskill and introduce new mechanisms to ensure effective and efficient oversight, strategic leadership and, ultimately, legitimacy for their organisation.

The latest trends in the profession have placed risk professionals in good stead, despite the pandemic. They are working more closely with their boards and senior management, and in collaboration with their colleagues in other functions within the organisation.

The Covid-19 situation is an opportunity for risk professionals to demonstrate the value of their work to their organisations. They are having more contact with their senior management and are more firmly embedded in what their organisations are doing.

A pandemic demands integrated enterprise risk management – a set of practices and processes underpinned by culture and technology, geared towards improving decision-making and performance through an integrated view of how well an organisation manages its own set of risks.

In responding to the Covid-19 crisis, agility combined with effective leadership is among the most important traits for risk professionals. This equips them in tackling the increasingly interconnected risks and megatrends today. This report has walked us through how risk professionals can navigate the five risk megatrend areas, as well as how insurance buyers, brokers and insurers can work together during times of crisis.

Resilience is more important than ever for organisations as they face a growing array of risks. Airmic's Resilience and Transformation Model lays out eight principles for achieving resilience and digital transformation, which can be summarised as follows:

1. The risk radar focused on emerging risks and developments in technology.
2. Resources and assets able to take full advantage of developments in technology.
3. Relationships and networks that are constantly developed and extended.
4. Rapid response supported by excellent communication within the organisation.
5. Review and adapt to events to protect and enhance reputation.
6. Redesign processes to embrace new technologies and encourage innovation.
7. Retain stakeholders during the transformation by analysing big data.
8. Reinvent purpose by opportunity awareness, commitment and capabilities.

As a recent INSEAD working paper *Crisis Management: Framework and Principles with Applications to Covid-19* points out, a crisis is not the time for learning or reinventing what should already be known. Rather, it is a time for experienced hands, endowed with healthy doses of science and intuition, to take charge.

These are not just lessons and fixes for the Covid-19 crisis, but for the future of risk management in the new normal.

Survey & research methodology

This report, produced by Airmic in collaboration with AIG, Control Risks, KPMG, QBE and Willis Towers Watson, is based on 150 responses gathered in a survey from 14 February to 31 March 2020. For context, this corresponded to the period when the Covid-19 pandemic was beginning to hit Europe, in particular from the first cases of infection in northern Italy until the end of the UK's first week of lockdown.

Subsequently, roundtables with Airmic members were held to gather qualitative responses. Written interviews were held with key representatives of the associations listed below in the acknowledgements.

Risk megatrends: ranking methodology

From a list of five risk megatrend areas with five sub-areas each, survey respondents were asked to assess the extent to which each of these would be of concern to them and their organisations, in the course of the next three years. They were asked to do so on a scale of 1 to 5, where 1 meant it was 'not a concern' and 5 meant it was of a 'very high concern'.

The list of megatrend areas and sub-areas was mapped out by Airmic and its five partners during of December 2019 and January 2020, and reinforced through secondary research and benchmarking with other risk megatrend studies. To reduce selection bias and to pre-empt unforeseen risk areas, survey respondents were also offered open-ended options to identify and assess other risk megatrends not on the list.

A simple average for the level of concern each risk megatrend sub-area posed to all respondents was calculated and expressed as a score out of 1 to 5.

The level of concern for any given risk can thus be formally denoted as:

$$\text{concern}_r = \frac{1}{N_r} \sum_{n=1}^{N_r} \text{concern}_{r,n}$$

where N_r is the number of respondents for risk r , and $\text{concern}_{(r,n)}$ is the level of concern assigned by respondent n to risk r . The level of concern felt by respondents to each risk was measured on a scale of 1 to 5.

Acknowledgements

We would like to thank all Airmic members and other organisations who have contributed their insights and thoughts to this report.

Airmic – Technical & Research team

Julia Graham
Deputy CEO and Technical Director
julia.graham@airmic.com

Hoe-Yeong Loke
Research Manager
hoeyeong.loke@airmic.com

About us



American International Group, Inc. (AIG) is a leading global insurance organization. AIG member companies provide a wide range of property casualty insurance, life insurance, retirement solutions, and other financial services to customers in more than 80 countries and jurisdictions. These diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security. AIG common stock is listed on the New York Stock Exchange. Additional information about AIG can be found at

www.aig.com | YouTube:
www.youtube.com/aig
 Twitter: @AIGinsurance
www.twitter.com/AIGinsurance
 LinkedIn: www.linkedin.com/company/aig



Control Risks is a specialist global risk consultancy that helps to create secure, compliant and resilient organisations in an age of ever-changing risk. Working across disciplines, technologies and geographies, everything we do is based on our belief that taking risks is essential to our clients' success. We provide our clients with the insight to focus resources and ensure they are prepared to resolve the issues and crises that occur in any ambitious global organisation. We go beyond problem-solving and provide the insight and intelligence needed to realise opportunities and grow.

www.controlrisks.com



KPMG in the UK is one of the largest member firms of KPMG's global network of firms providing audit, tax and advisory services. In the UK we have 631 partners and 15,864 outstanding people working together to deliver value to our clients across our 22 offices. Our vision is to be the clear choice in professional services in the UK. For our clients, for our people and for the communities in which we work. KPMG's core business is to help your organisation work smarter, evaluate risks and regulation and find efficiencies. We do this by providing deep insight into market issues, transparency in everything we do, and using innovative technology to tackle complex problems. We are focused on the issues that keep our clients awake at night and responding to them as One Firm. To do that, we strive to create a high performance culture, guided by our values, where our diverse talent feels included and excels.



QBE is a specialist business insurer and reinsurer. We're big enough to make a difference, small enough to be fleet of foot. We may not be the best known, but a large part of the modern world depends on our cover. We have clients as varied as bus and coach fleet drivers and major international infrastructure consortiums. For them, we're the buffer between the best-laid plans and uncertain reality. People who deal with us find us professional, pragmatic and reliable – this is one of the reasons we're still here after 130 years. Our underwriters are empowered to take decisions that are important to you. (Because we know no computer can replace that human ability.) And we don't just cover your risk. We help you manage it, meaning that you're less likely to have to make a claim in the first place.

QBE European Operations
Tel +44 (0)20 7105 4000
www.QBEurope.com



Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 45,000 employees serving more than 140 countries and markets. We design and deliver solutions that manage risk, optimise benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at

willistowerswatson.com



Marlow House
1a Lloyd's Avenue
London
EC3N 3AA

Tel: +44 207 680 3088
Fax: +44 207 702 3752
Email: enquiries@airmic.com
Web: www.airmic.com