

# ALLEN & OVERY

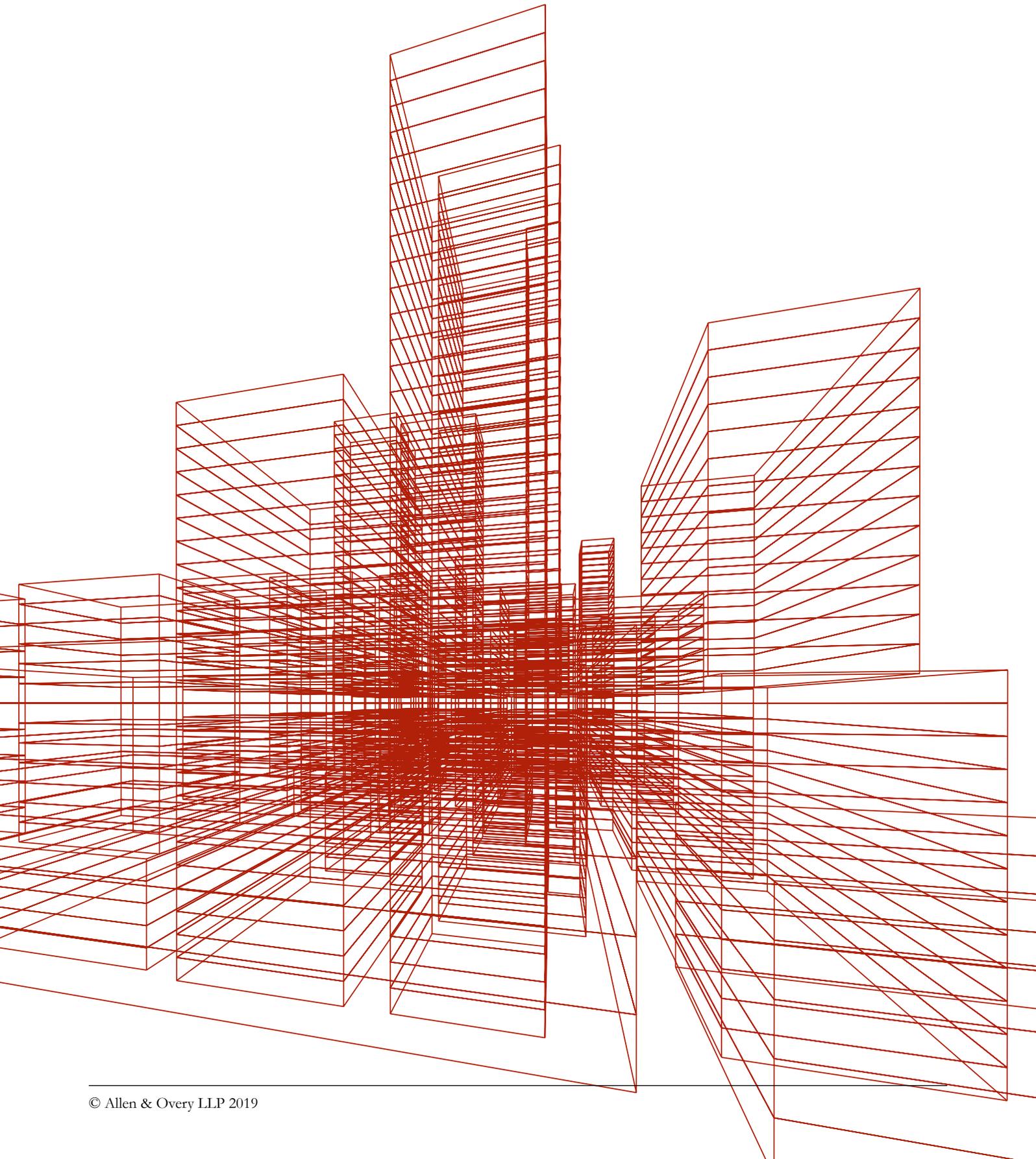
Willis Towers Watson 

## Directors' Liability Report

*D&O: A new era of risk exposure*

---

A survey and review of the legal and regulatory landscape  
Conducted by Allen & Overy LLP and Willis Towers Watson  
2019/2020



# Contents

Introduction	04
Executive summary	07
Key findings	08
The changing face of global risk	10
– <i>Exposure in uncertain times</i>	10
– <i>Corporate culture</i>	11
– <i>Climate change and community impact</i>	12
– <i>Modern slavery and human rights</i>	13
– <i>Sanctions regimes</i>	14
Addressing personal exposure	15
– <i>Senior Managers and Certification Regime and individual accountability regimes</i>	16
– <i>The Auditing, Reporting and Governance Authority</i>	17
– <i>Litigation risk – the global growth of class actions and related funding mechanisms</i>	17
– <i>Employment claims</i>	18
– <i>Insolvency risk</i>	19
Cyber security and data risk	20
– <i>Data risks</i>	21
– <i>Technological risks</i>	22
Protecting directors and officers	24
A guide: practical tips on D&O and indemnities	27

# Introduction

Welcome to this seventh edition of our annual series looking at directors' liabilities, in which we explore the ever-expanding personal accountability faced by company directors at a time when regulators and enforcement agencies continue to have management in their sights. We began this exercise in 2011, as a joint effort by international law firm Allen & Overy LLP and the global risk management brokerage and advisory firm Willis Towers Watson. This was immediate aftermath of the global financial crisis, and the trend towards holding directors and officers personally to account has only grown since.

In this year's survey we have cast our net far wider than ever before, interviewing 252 directors, non-executive directors, partners, in-house lawyers, risk officers and compliance professionals all over the world. Half of our respondents work in listed companies, while 87% are in businesses employing more than 500 people and 40% in firms employing more than 5,000 people. Eight years on from our first survey, this year's responses paint a picture of heightened anxiety and exposure, with more and more individuals having direct experience of a claim or investigation involving a director in their business. As in previous years, the results indicate that regulatory claims and investigations are becoming more common and that individuals feel more exposed. Respondents in over half of listed companies have experience of such an incident: that figure rises to 60% in the finance, insurance and real estate industry.

This year, two "Cs" – cyber and culture issues – head the list of issues troubling directors. To this we would add a third "C" – climate change – which is fast moving to the top of the agenda of boards.

## Cyber

---

When considering cyber, it is the fear of the impact of incidents of cyber attacks or data breaches that is increasingly centre stage. For the first time, more than half of our respondents report direct experience of either a significant cyber attack or a sizeable data loss in the past 12 months, up from 44% last year to 54%. For the second consecutive year, the risks associated with cyber security and data loss lead the list of business risks that directors are most concerned about, ahead of regulatory, litigation and criminal exposures. What's more, technological advances more broadly are now also giving rise to growing liability concerns, with more than half of respondents worried about risks associated with artificial intelligence and machine learning.

## Culture

---

The global conversation about corporate culture and the way in which ethics have contributed to many of the systemic failures in the financial services industry and elsewhere is gathering speed. In February 2019, the Australian Royal Commission into Misconduct in the Financial Services Industry was just the latest to weigh in on the need for entities to take proper steps to assess and improve the cultures of their organisations. The UK's Financial Conduct Authority (the FCA) has been a trailblazer on this issue, with regulators in Hong Kong and Singapore also taking action to address matters of corporate values, governance and incentivisation.

Directors are now in the firing line not only for their own behaviour, but for failing to do more to drive widespread good conduct throughout their businesses. In our survey, respondents say they are broadly confident that they understand their organisation's culture, but less confident that that culture matches up to the business's stated values or that they have an ability to change the culture if required. This, we expect, will become a key focus of attention for regulators and claimants.

The challenge in driving good culture may be what lies behind the fact that both litigation risk and reputational risk feature high in the list of director concerns. For the first time, in 2019 both appear in the top five legal, regulatory and business risks that are worrying respondents.

## Climate Change

---

When it comes to climate change, there continues to be a level of concern reflected in our survey responses. Although to date no companies have been found liable for the effects of climate change, let alone any directors and officers, this does not mean that the costs of defending these claims have not made an impact on D&O liability insurance policies. Globally, it is estimated that there are now 1,300 climate change claims in 28 countries. It is therefore unsurprising that this is a growing worry for directors.

Turning to D&O protection and the role of insurance in settling the minds of respondents, there is increasing evidence of directors wishing to be more actively engaged in issues that may have an impact on their ability to respond to a claim. The control and settlement of claims is now the number one concern to our interviewees, having moved up the agenda significantly in recent years, with the way in which individuals can access, and control access to, the policy also featuring highly. Today, two-thirds of respondents say they understand the liability protection available to them, and that figure rises to one in four of those in listed companies. As the risk landscape continues to evolve, it is encouraging to see growing engagement and awareness from respondents about the D&O protections available.

We turn in the final section of this report to the ways in which directors can ensure their D&O policies can be crafted to provide the right protection but, by way of example, proper D&O cover is vital for directors who agree to accept appointments on client boards as bankers sometimes do or on subsidiaries and joint venture companies not wholly owned by the parent company; such potential gaps in cover can prove very problematic.

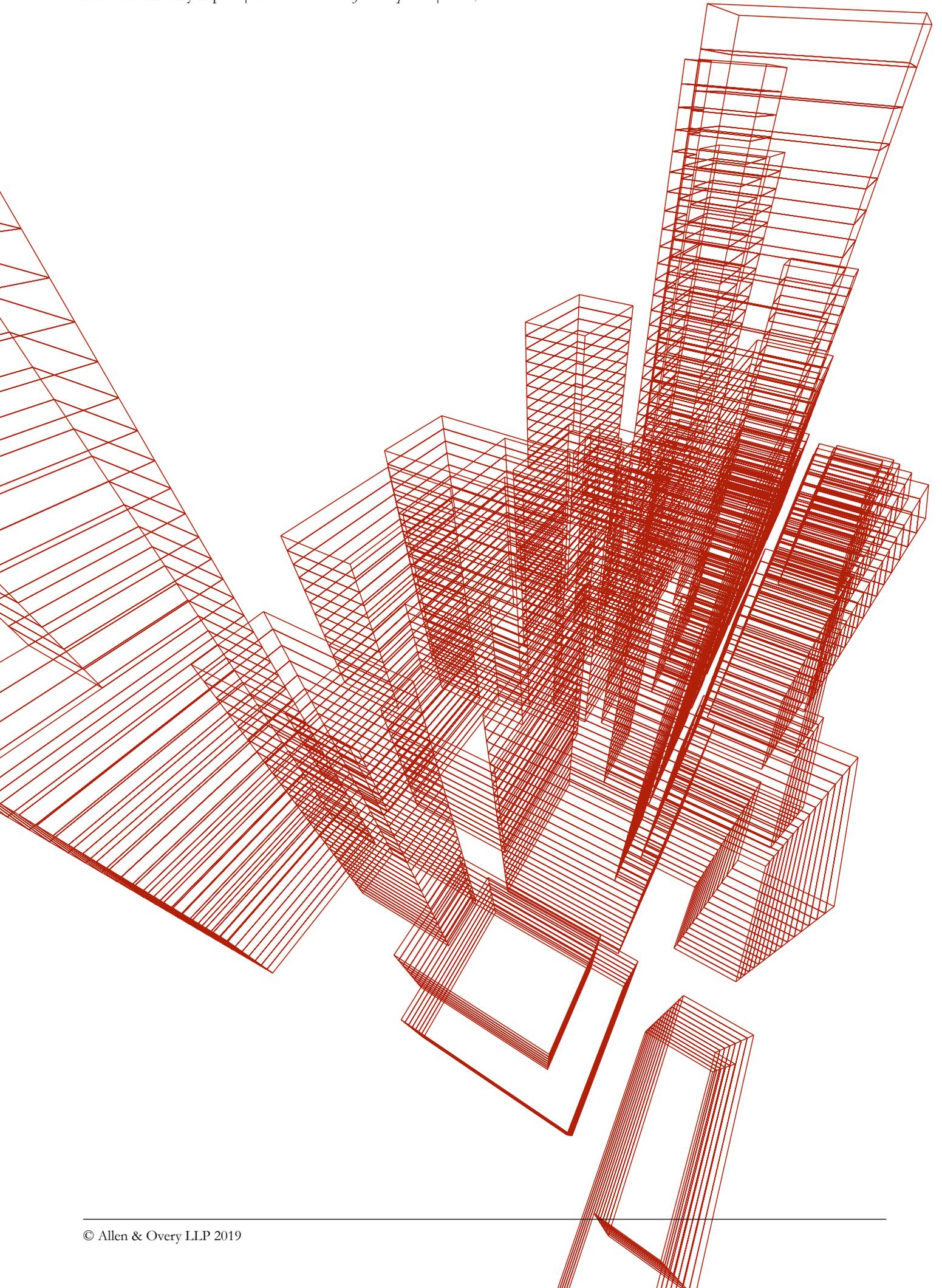
We hope that the coverage and analysis over the following pages proves useful and insightful. Should you require any additional information or wish to discuss any of the issues raised here, please do not hesitate to get in touch with your usual contact at either Allen & Overy or Willis Towers Watson.



**Joanna Page**  
Partner, Allen & Overy  
[joanna.page@allenovery.com](mailto:joanna.page@allenovery.com)



**Francis Kean**  
Executive Director,  
Willis Towers Watson  
[francis.kean@willistowerswatson.com](mailto:francis.kean@willistowerswatson.com)



# Executive summary



Almost half of all respondents have **experienced a claim or investigation** involving a director in the past 12 months, and that number is increasing year on year



More than half of respondents have **experienced a cyber attack or loss of data** significant enough to come to the attention of the board, and again this is increasing year on year



Technological advances and risks associated with **artificial intelligence and machine learning** are consistently identified as one of the most significant global risks



**Data loss** is identified as the most significant legal, regulatory or business risk, closely followed by cyber attack



Nearly all respondents claim to understand their organisation's **corporate culture** but only half believe they can influence or change it



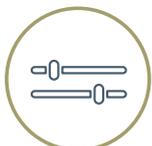
As we become used to a new normal of uncertainty, geo-political and economic concerns have reduced slightly as a very significant or extremely significant concern. Instead, **climate change has moved up the ranks** – 40% of respondents rated it as very significant or extremely significant concern



There is a growing awareness of the role of litigation funders in driving large-scale actions, including class actions, and for the first time nearly half of respondents consider **litigation risk** to be high



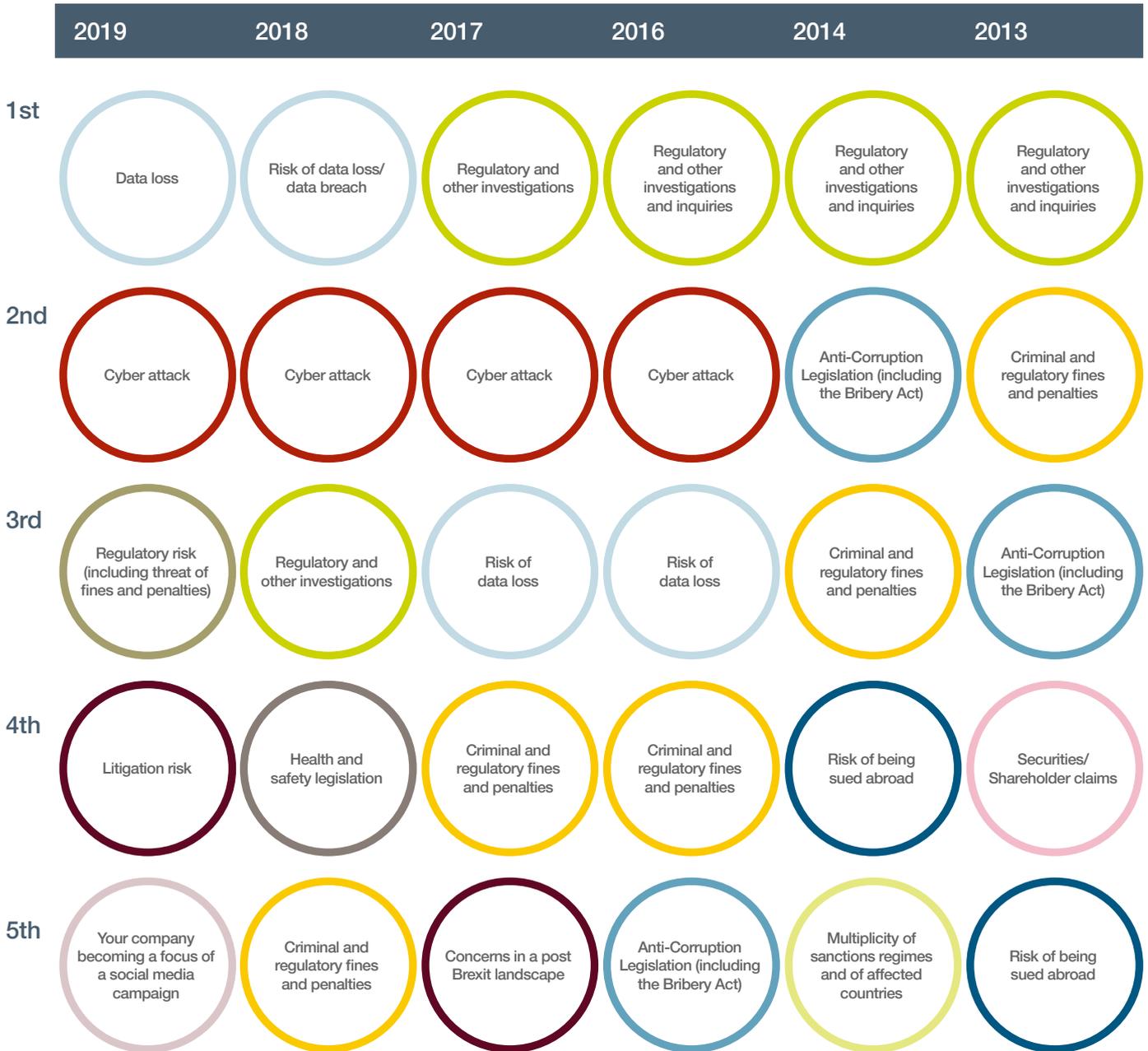
**Civil proceedings brought by third parties** are identified as the most significant personal risk



For the first time in seven years the top threshold insurance coverage issue for directors is **how claims against them will be controlled and settled**

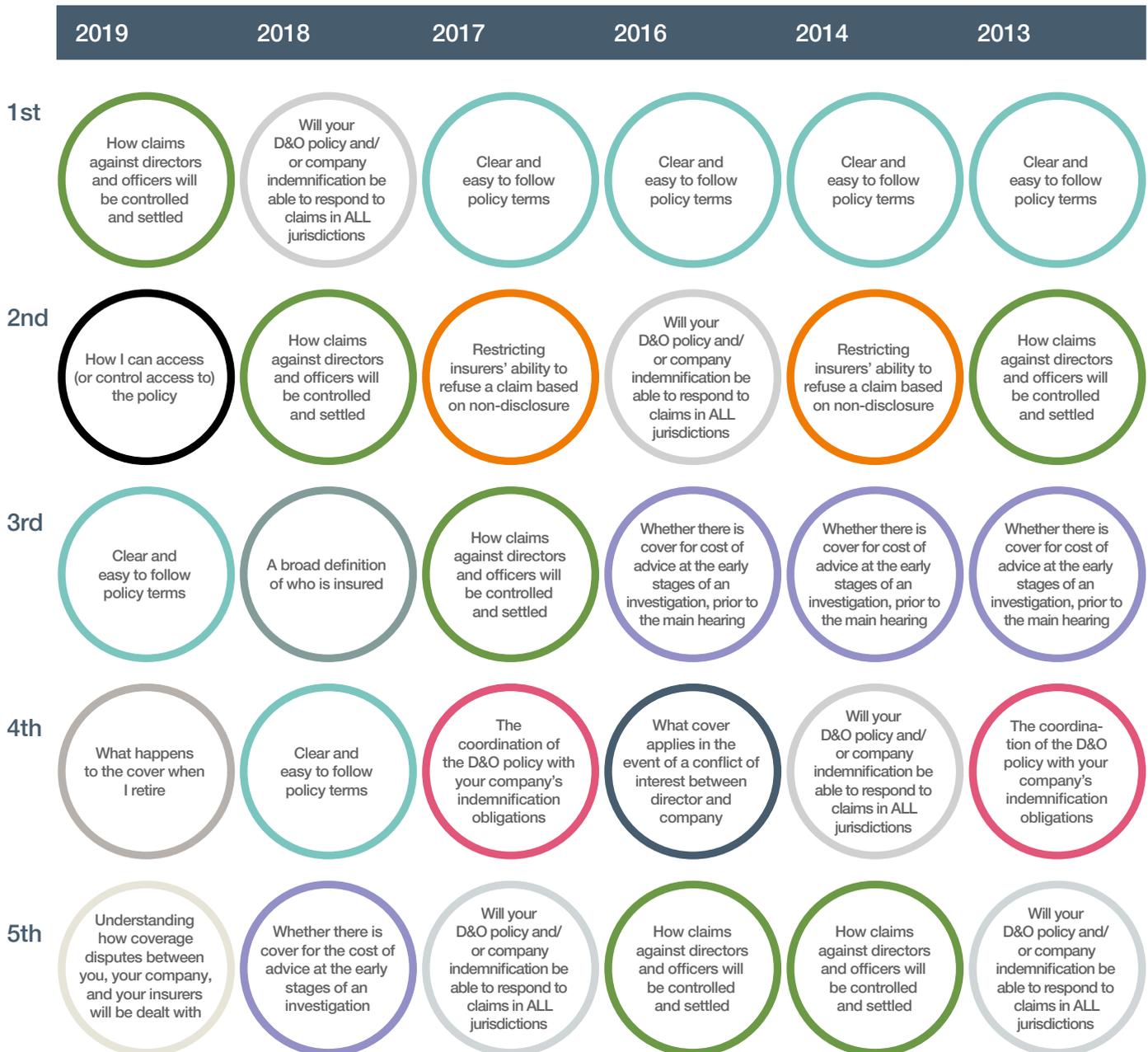
# Key findings

## Top five legal, regulatory and business risks, year-on-year\*



\*Note: there was no 2015 report

## Top five threshold and coverage issues of liability insurance, year-on-year\*



\*Note: there was no 2015 report

# The changing face of global risk

## Exposure in uncertain times

---

Last year, we asked our respondents about the risks being placed on their operations as a result of the global economic climate. Some 68% told us that economic conditions were creating a new level of risk, just as two-thirds also pointed to challenges created by geopolitical uncertainties. This year, those worries have not gone away, but they no longer dominate to the same extent (although the fact that a greater proportion of our respondents are now outside Europe may also influence these findings).

In 2019, 48% consider the economic climate to pose a very or extremely significant risk to their business operations, while 46% say the same about the geopolitical climate. These figures are highest amongst respondents in listed companies, where 60% are extremely worried about the economy for example, and in the UK, where 56% and 51% are very concerned about economics and geopolitics respectively.

The slightly reduced emphasis on economic risk is something of a surprise. But perhaps it reflects the number and complexity of risks clamouring for attention. According to the World Economic Forum's Global Risks Report 2019, it was in fact macroeconomic risks that moved into sharper focus last year, as financial markets' volatility increased. Likewise, geopolitical and geo-economic tensions rose among the world's major powers, most notably through the trade war between the U.S. and China. These tensions seem to represent some of the most urgent global risks at present.

The same report points to environmental risks dominating global concerns, and also highlights technology as continuing to play a profound role in shaping the global risk landscape. At a corporate level, technological advances rank highest in the list of global risks on the minds of directors and officers, with 58% considering the risks associated with artificial intelligence and machine learning to be very or extremely significant for their company's business operations.

*“Risks associated with health and safety, climate change, human rights and community impact are moving up the agenda”*

For business leaders, this backdrop of risk heightens the concerns about operating internationally, and there are a raft of issues that serve only to increase these worries, including the difficulties associated with dealing with multiple sanctions regimes, with navigating antitrust laws across borders and with compliance with bribery and corruption legislation.

In the U.S., a case involving Toshiba has found that companies can face class actions where their securities are traded as unsponsored Level 1 ADRs (American Depositary Receipts, which are instruments not listed in the U.S. but traded over the counter). The U.S. Court of Appeals for the Ninth Circuit found that, even though such ADRs can in theory be traded without the company's knowledge or consent, the company and its directors can still be sued in the U.S. The UK government submitted an amicus brief in the proceedings stating that, “this appeal involves a particularly alarming example of interference with a foreign national's legal system... [which will] allow private U.S. plaintiffs to undermine a foreign government's usual regulation of its domestic securities market even when a foreign-registered company's own activities have no factual nexus to the United States”.

A further concern is the extent to which a UK-based parent company can be held legally responsible for the actions of its foreign subsidiaries. The 2012 case of *Chandler - v - Cape Plc* in the English courts has some significance for main board directors. This case had already established circumstances in which it is right to attach legal responsibility to a parent company for the welfare of the employees of its subsidiaries, but an April 2019 judgment from the UK's Supreme Court further sets out that the UK may be an appropriate jurisdiction in which to bring such claims against UK-based parent companies, even where the relevant subsidiary and the damage complained of took place abroad.

The April 2019 judgment concerned alleged toxic emissions from a copper mine in the Chingola District of Zambia and could have profound implications for UK boards. The claimants were 2,000 Zambian citizens who brought the case to the UK, arguing that the company's group-wide quality control, environmental impact and management policies effectively created a duty of care on the parent to ensure those policies were complied with. The Supreme Court judgment does not attempt to categorise the types of situation in which claims like this might be possible, and therefore establishes a principle that liability is at least sometimes legally arguable.

Against a backdrop of legal decisions such as these, which retrospectively rewrite the liability landscape for companies and their directors, it is hardly surprising that directors are troubled as to the level of their potential exposure.

## Corporate culture

Whether addressing legal, regulatory, criminal, global or personal risks, directors and officers need to be comfortable that the culture of the organisation in which they are operating matches the stated values and prioritises both good behaviour and compliance. Weak and unethical cultures have been blamed for many of the systemic failures in the financial services industry and beyond in the past decade, and regulators are increasingly focused on corporate culture as a means to improve behaviours and outcomes more broadly.

Against this backdrop, we asked respondents to this year's survey a series of questions about corporate culture, finding that 83% believe they understand their organisation's culture, but only 74% believe the corporate culture matches the company's stated values. Perhaps more concerning, however, is the fact that only 59% of business leaders believe they can change their organisation's culture, with this figure rising to 67% in listed companies.

This is a growing area of risk management as the importance of good culture moves up the regulatory and enforcement agenda. Banks, national sports teams and car manufacturers have all been in the spotlight in recent years for deep cultural failings that have led to widespread reputational damage, and financial services regulators globally have brought increasing focus on the way that senior leaders define and reinforce the firm's culture to drive the behaviours expected at all levels of the organisation.

*“Banks, national sports teams and car manufacturers have all been in the spotlight in recent years for deep cultural failings that have led to widespread reputational damage”*

Ten years have passed since the financial crisis, and the UK's FCA continues to focus on its long-held belief in tackling conduct issues through culture. The number of FCA enforcement investigations into issues relating to culture and governance has

increased by 1,066% in the last three years and the topic continues to gather pace globally, most recently in Australia where a Royal Commission review has found widespread misconduct in financial services.

*“FCA enforcement investigations into issues relating to culture and governance has increased by 1,066%”*

In February 2019, Australia's Commissioner Kenneth Hayne released his final report following the Royal Commission, which fundamentally forces organisations to re-examine their purpose, which should not be all about profit, and place an even stronger focus on the need for a robust culture to underpin the right actions. The report made 76 recommendations challenging key aspects of the financial services industry, including recommending a heightened focus on culture and governance. Recommendations included that all financial services companies review the design and features of their remuneration systems for frontline staff and assess their own culture and governance at least once a year. There is also the potential that the Banking Executives Accountability Regime, currently in place for Australian Authorised Deposit Taking Institutions and their senior executives and directors, will be extended to all APRA-regulated financial services companies.

According to Theresa Lewin, Financial Institutions Industry Leader Australasia, and Pat Bibb, Senior Consultant, Talent & Reward, at Willis Towers Watson: “A note of caution is appropriate given that a broader range of stakeholders than has ever been the case will be carefully examining these assessments and organisational practices and making judgements on whether or not the culture and risk management frameworks are both robust enough and functioning as intended. What has typically been held as sufficient in this domain in the past, a tick-box exercise, will no longer be sufficient as stakeholders and regulators will seek real written and practical evidence of the proactive management of the broadest range of risk.”



Theresa Lewin



Pat Bibb

*“What has typically been held as sufficient in this domain in the past, a tick-box exercise, will no longer be sufficient as stakeholders and regulators will seek real written and practical evidence of the proactive management of the broadest range of risk.”*

Theresa Lewin, Financial Institutions Industry Leader, Australasia and Pat Bibb, Senior Consultant, Talent & Reward, at Willis Towers Watson

They add: "This will need to be supported by a transparent and deliberately managed culture, strengthened governance and risk capability across the organisation, an appropriate remuneration framework, significantly improved interaction between the board and senior management and better functioning of, and interaction between, a variety of board committees – which together set the 'tone from the top'."

Lee Alam, Asia Pacific head of A&O Consulting, adds: "The cultural shift across the Australian financial services sector will take many years. It starts by boards and senior executives accepting that change is needed and personally driving enhancements to culture and conduct, through the way they define organisational values and ensure that the way the firm does business each day lives up to those values."

Risk culture is part of the broader organisational culture. It reflects the way attitudes and beliefs are displayed when individuals in an

organisation ignore, take or manage risks. Without a strong ethical culture, organisations will always be at risk. If the culture of an organisation does not support principled performance, then all the people, processes and technologies that are implemented to mitigate ethics and compliance risks are unlikely to be effective.

Sally Dewar, CEO of A&O Consulting, says: "Having a clear organisational purpose, bolstered by a set of core values and supported by consistent messaging, is just the start."

A robust risk management framework – appropriately designed, positioned and resourced – will survive executive changes at the top of the organisation. A positive culture with integrity at its core is the foundation for an effective risk culture which, when properly embedded throughout the organisation, can create a significant competitive advantage and serve as a valuable organisational asset.



*"The cultural shift across the Australian financial services sector will take many years. It starts by boards and senior executives accepting that change is needed and personally driving enhancements to culture and conduct, through the way they define organisational values and ensure that the way the firm does business each day lives up to those values."*

Lee Alam, Managing Director – A&O Consulting, Sydney

## Climate change and community impact

Another area of growing concern for directors and officers is around climate change and community impact, with 40% of our respondents either very or extremely worried about the potential for environment and climate change to impact on business operations. This concern is highest among large firms (46%), listed companies (49%), and those based in the UK (43%, compared to 32% for those based in Australia).

There is certainly growing evidence of regulators holding senior managers to account for financial risks associated with climate change, with the UK's Prudential Regulation Authority (PRA) publishing a supervisory statement, SS3/19, in April 2019 that requires banks and insurance companies to have in place from October 2019 updated senior management function forms addressing the issue. The PRA says that few firms are taking a strategic approach to considering how actions today will affect future financial risks, and it therefore expects firms to have clear roles and responsibilities for the board and its sub-committees in managing risks from climate change.

It is now up to banks and insurers to decide on a senior manager to assume responsibility for climate risk, which raises the question of whether organisations will have the appropriate level of climate expertise in house to deal with the issue. The supervisory statement draws a distinction between the physical and the transitional risks associated with climate change, with the first covering the effects of extreme weather events and longer-term climate shifts, while the latter looks at risks associated with adjustment to climate change, such as policy and regulatory change and disruptive technology.

While climate change litigation has so far been less successful than some had predicted, it would be wrong to assume the risk is limited to obvious sectors like energy and transportation. This regulatory focus specifically on the financial risks for banks and insurers highlights that all directors are right to be concerned about the issue.

## Modern slavery and human rights

---

The trend towards increased regulation and scrutiny of the human rights impacts of corporations continues across the world, with the court of public opinion – often emboldened by social media – arguing its case that human rights breaches are occurring as a result of sponsorship and/or funding that derives from companies in the developed world.

In this year's survey, directors and officers are concerned about the risks associated with breaches of human rights within their business operations, with one in three describing such a risk as very or extremely significant. In particular, supply chain exposure, where corporates are not able to assess the working conditions of every person in their supply chain, can be a huge risk. Worry about the issue appears highest in the services, hotel and leisure sector, where 41% consider human rights a very real concern.

*“Directors and officers are concerned about the risks associated with breaches of human rights within their business operations”*

The UK's Modern Slavery Act 2015 is designed to combat modern slavery in the UK and includes a supply chain clause, compelling larger businesses to make public their efforts to stop the use of slave labour by their suppliers. Heralded as the first legislation of its kind worldwide, and thought to have inspired other governments to introduce their own supply chain transparency and due diligence laws, the UK government has now published an independent review and recognised that its legal obligations need to be backed up by more effective enforcement mechanisms and penalties. Of the 17,000 organisations thought to be required to produce a modern slavery statement under the Act, only around 60% are thought to have done so, and many are of poor quality.

In July 2019, it was announced that the government will consult on adding more teeth to the modern slavery requirements in the UK, including the gradual introduction of an enforcement mechanism with the option of civil penalties as a percentage of turnover.

The number of live police operations into modern slavery in the UK has increased from 188 in December 2016 to over 1,370 today, while in the year to September 2018, 4,270 offences of Modern Slavery were recorded by police, a 51% increase on the previous year. Given the importance of brand and reputation to large companies, and the emotionally charged press reports of people trafficking and slavery rings, this is an issue upon which managers are increasingly focused.

## Sanctions regimes

The risk of a breach of sanctions continues to feature reasonably highly on the list of personal risks that concern senior business leaders. In all, 34% say the risk of a breach is a very or extremely significant risk for them personally, a figure that rises to 42% for those working in listed companies and to 41% for those working in services, hotels and leisure.

Russia remains a particularly difficult market in which to operate following the introduction of EU-U.S. sanctions in 2014, in response to the annexation of Crimea and the crisis in eastern Ukraine. Broadly such sanctions target individuals, major Russian state banks and a list of corporations, while restricting access to EU-U.S. capital markets and halting some western imports of high-tech goods. But there are differences between the U.S. and European sanctions policies that make them difficult to navigate, with Washington targeting oil and gas players, for example, while Europe focuses on oil.

In November 2018, the U.S. imposed sanctions on 700 Iranian targets (focusing on the oil, financial and shipping sectors) – the toughest sanctions ever imposed on Iran. In September 2019, further economic sanctions were announced against the country by President Trump,

targeting the Central Bank of Iran and its sovereign wealth fund as part of an effort to cut off funding of global terrorism and end the domestic oppression of the Iranian people.

The sanctions landscape generally remains complex and a difficult environment against which to conduct business. The recent (brief) imposition and the lifting of sanctions relating to Turkey illustrates the difficulties facing companies working to keep pace with unpredictable political policies.

In the UK, the Sanctions and Anti-Money Laundering Act 2018 is meant to allow the UK to maintain the status quo after it leaves the EU in respect of both sanctions and anti-money laundering (AML), but it also creates powers for the UK to impose its own sanctions and AML measures post-Brexit. While it does not come into effect until the UK leaves the EU and is no longer subject to EU law in these areas, it does create a risk that the UK will diverge from existing EU regimes in due course. All UK businesses and executives, and particularly those working in financial institutions, will need to be mindful of this going forward.

### France's new Law PACTE

Directors of French companies are now also being called upon to ensure that their companies respect social and environmental values, which includes respecting human rights and preserving biodiversity. The new Law PACTE imposes wider obligations on directors, including a requirement to declare a *raison d'être*, which is a statement of values that the company intends to promote in the achievement of its corporate purpose.

# Addressing personal exposure

The regulatory focus on individuals that began to emerge in the wake of the global financial crisis and has continued to gather pace in the following decade continues to have a significant impact on directors and their perceptions of risk. This year, as in previous years, the results of the survey indicate that regulatory claims or investigations against company directors are becoming more common, with 42% of respondents having experienced regulatory claims involving leaders of their companies in the past 12 months.

The chances of respondents having experienced a regulatory claim correlate to the size of their business, with 45% of those working in large companies having done so compared to 38% of those working in businesses with fewer than 500 employees. Furthermore, the incidence is higher in listed companies than it is in private firms – 52% versus 40% – and is highest for those working in European offices (excluding the UK), where 48% have seen a regulatory claim or investigation against a director compared to 37% in the UK and 40% in Australia.

Perhaps unsurprisingly, it is in financial services where the regulatory activity is strongest, and in finance, insurance and real estate we found 60% of respondents reporting experience of a claim or investigation involving one of their directors. The sectors least impacted include services, hotels and leisure, government and public institutions, and industrial and manufacturing.

Tracking these responses over time, it is immediately apparent that claims and investigations involving directors are increasing year on year, and when both criminal and regulatory claims are taken into account, we see 49% of respondents reporting experience of a claim or investigation involving a director this year compared to just 27% in 2016 and 34% last year. Such experiences translate into real concern – this year, exactly half of our respondents felt that the regulatory risk, including the threat of fines and penalties, was either very or extremely significant, and a further 37% felt the same exposure to criminal proceedings.

Culture plays an important part here too. An individual's contribution to establishing the right corporate culture is increasingly under the spotlight for regulators, for example in relation to reliance which can be placed by a company in establishing the defence of adequate procedures to prevent bribery.

## Senior Managers and Certification Regime and individual accountability regimes

In force since March 2016, the UK's Senior Managers and Certification Regime (SMCR) for banks, building societies and a small number of investment firms is designed to improve governance and accountability by focusing on individuals. Over the course of its three years, the reach of the SMCR has gradually expanded, with insurance and reinsurance firms regulated by the FCA and the PRA covered since December 2018 and all firms authorised by the FCA under its remit since 9 December 2019.

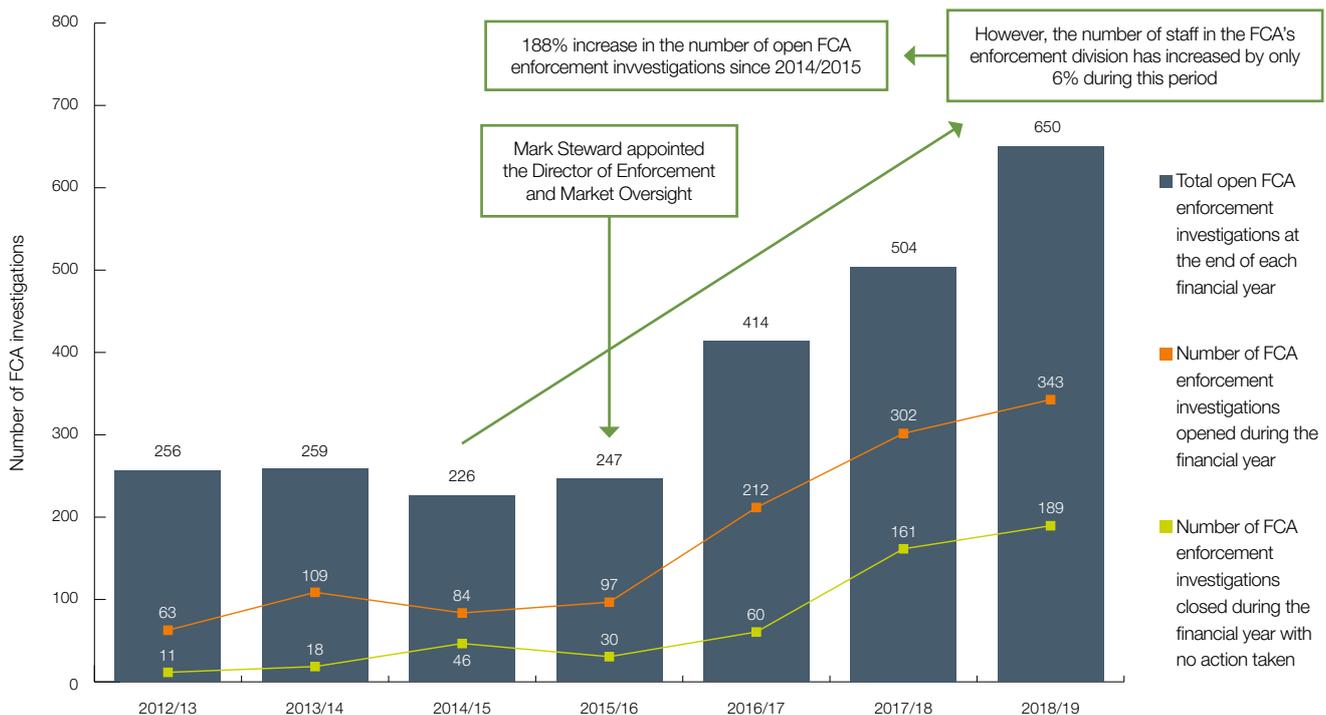
The SMCR has at its heart a focus on reducing harm to consumers and strengthening market integrity by making individuals accountable for the conduct and competence of the business. It aims to encourage a culture of staff at all levels taking personal responsibility, and to make sure firms and staff clearly understand and can demonstrate where responsibility lies. The FCA is currently opening more cases than ever before, with a particular focus on financial crime. At the end of the financial year 2018/2019, the FCA had 650 open enforcement investigations, compared to 504 the year before, representing a 188% increase since 2014/2015. Investigations into individuals represent about 19% of all current FCA enforcement investigations, according to a Freedom of Information request.

*“At the end of the financial year 2018/2019, the FCA had 650 open enforcement investigations, compared to 504 the year before, representing a 188% increase since 2014/2015”*

Similarly, since April 2013, the PRA has also opened 49 investigations into 22 different matters, looking into 17 firms and 32 individuals. Six investigations have resulted in enforcement action against individuals.

Alongside the SMCR, individual accountability regimes continue to gain weight around the world. While the United States has no formal individual accountability regime, in November 2018 the Federal Reserve Board adopted a new rating system for large financial institutions that includes supervisory expectations for senior management, business line management and independent risk management. Elsewhere, Hong Kong's new Management Accountability Initiative came into force in March 2018 and Australia's Banking Executives Accountability Regime for large authorised deposit-taking institutions came in on 1 July 2018 and was extended to small and medium-sized institutions in 2019, with proposals on the table to further extend the regime to all other financial services firms.

Singapore has been consulting on proposed guidelines on Individual Accountability and Conduct since last year; Malaysia has been discussing a new regime since February 2018; and in Ireland, proposals for a Senior Executive Accountability Regime were announced in July 2018.



Sources: FCA Annual Reports and Freedom of Information Act request

## The Auditing, Reporting and Governance Authority

---

Concerns about the effectiveness of the Financial Reporting Council (FRC) in the UK, which currently acts as a watchdog for auditors and the guardian of the Corporate Governance Code, were first expressed by the House of Commons two years ago. A number of high-profile corporate collapses last year increased the pressure on the FRC, leading to the publication in December 2018 of a report by Sir John Kingman that was critical of the FRC's role and led to plans to abolish it and replace it with a tougher, more independent body with wider powers.

This new body, to be known as the Auditing, Reporting and Governance Authority (ARGA), will have jurisdiction over all CEOs, CFOs, Chairs and Audit Committee Chairs, and over all company directors with an accounting qualification. Directors will be responsible for certifying the material accuracy of financial statements and the effectiveness of internal controls, along similar lines to the Sarbanes-Oxley Act in the U.S.

The extent of ARGAs enforcement powers is yet to be revealed, but the Kingman Review did set out plans to hold directors to account for their duties to prepare and approve true and fair accounts and compliant corporate reports. While the power to disqualify directors will remain with the Insolvency Service, ARGAs may have the necessary powers to investigate directors and refer cases to them.

Given the UK government's stated plan to make ARGAs more interventionist and prescriptive than the FRC, this looks like a further tightening of the pressure on board members, who may now find it harder to raise a defence that they did not have the necessary accounting qualifications to understand a technical issue.

The implementation of the new regime, and the establishment of ARGAs, requires primary legislation and as such it is not possible to predict when it will come into being.

*“Directors will be responsible for certifying the material accuracy of financial statements and the effectiveness of internal controls”*

## Litigation risk – the global growth of class actions and related funding mechanisms

---

When it comes to the risks to which our respondents feel personally most exposed, it is notable that civil proceedings brought by third parties are now the most significant concern. Some 38% of respondents point to the risk of civil proceedings against them as the biggest risk to them personally, with that figure rising to 45% amongst respondents working in listed companies. The industries most concerned about the threat of litigation are financial, insurance and real estate (42%) and services, hotels and leisure (50%), while only 21% of those working in wholesale, retail and consumer goods perceive the threat of civil lawsuits to be a concern to them personally.

Aligned to this threat of civil proceedings against individuals is the changing litigation environment more generally, where the majority of those interviewed are now aware of the fact that large scale actions, including class actions, are being funded by litigation funders. In all, two thirds of our respondents report an awareness of the new litigation landscape, though fewer than half – 47% – consider this to be a risk to their business. Awareness is highest among large companies (69%) and listed businesses (78%), and there is a corresponding increase in concern in line with that awareness, with 53% and 55% respectively believing the advent of litigation funders to be a risk to their business.

In Germany, the continuing trend towards holding directors accountable has seen them very much in the spotlight in the ongoing diesel emissions scandal. Hundreds of thousands of German consumers are bringing a landmark legal action against Volkswagen over claims of emissions test cheating, in a case being led by the Federation of German Consumer Organisations (VZBV). That case is a declaratory model action, a new form of German legal instrument, similar to the U.S. class action, created to allow collective actions by consumers.

Class action legislation has also been extended in France, having first been introduced in 2014 with limited application. Now class actions can be brought in the country on matters of health product liability, environmental liability, personal data protection and discrimination.

So far as the UK is concerned, this finding is a little unusual since the new litigation funding environment has not so far produced an increase in civil litigation from third parties. Perhaps the fact that funding is very much in the news has instead served to create a greater awareness of risk. Geographically, the risk is considered highest in Continental Europe (57%) and lowest in Australia (33%), which again is unexpected given the prevalence of litigation funders in Australia. Industry-wise, the sectors that are most worried about litigation risk include financial services (58%) and services, hotels and leisure (53%).

## Employment claims

Employment claims have been in the spotlight ever since the global #MeToo campaign against harassment and sexual discrimination in the workplace began to take shape in 2017. Since then, the level of concern among our respondents about workplace issues – including pay, discrimination and #MeToo – has steadily increased, with 22% of respondents considering employment practice claims to be very or extremely significant risks in 2017, rising to 30% in 2018 and 35% this year.

The growing pressure to call out inappropriate behaviour in the workplace continues to gather pace, and many large law firms, financial institutions and corporates have been caught up in unfavourable headlines as a result of poor conduct or a failure to properly manage complaints. In July 2019, the Solicitors Regulation Authority (SRA) revealed that it had received 70 complaints about sexual harassment against solicitors in the previous 12 months, having received only 30 such complaints in the five years from 2012 to 2017. More than 80 hearing days were set aside by the Solicitors Disciplinary Tribunal this year to hear 25 cases of alleged sexual harassment and assault at law firms, according to the SRA's latest Upholding Professional Standards report, and the legal profession is not alone in dealing with such a deluge of new cases.

Workplace issues are of the greatest concern in listed companies, where 43% consider the risk significant as against just 25% in private firms. In the UK, 38% of respondents are significantly concerned, against 33% in the rest of Europe, while the industry sectors that are most worried include telecommunications, media and technology and services, hotels and leisure, where 47% express significant concern in both cases.

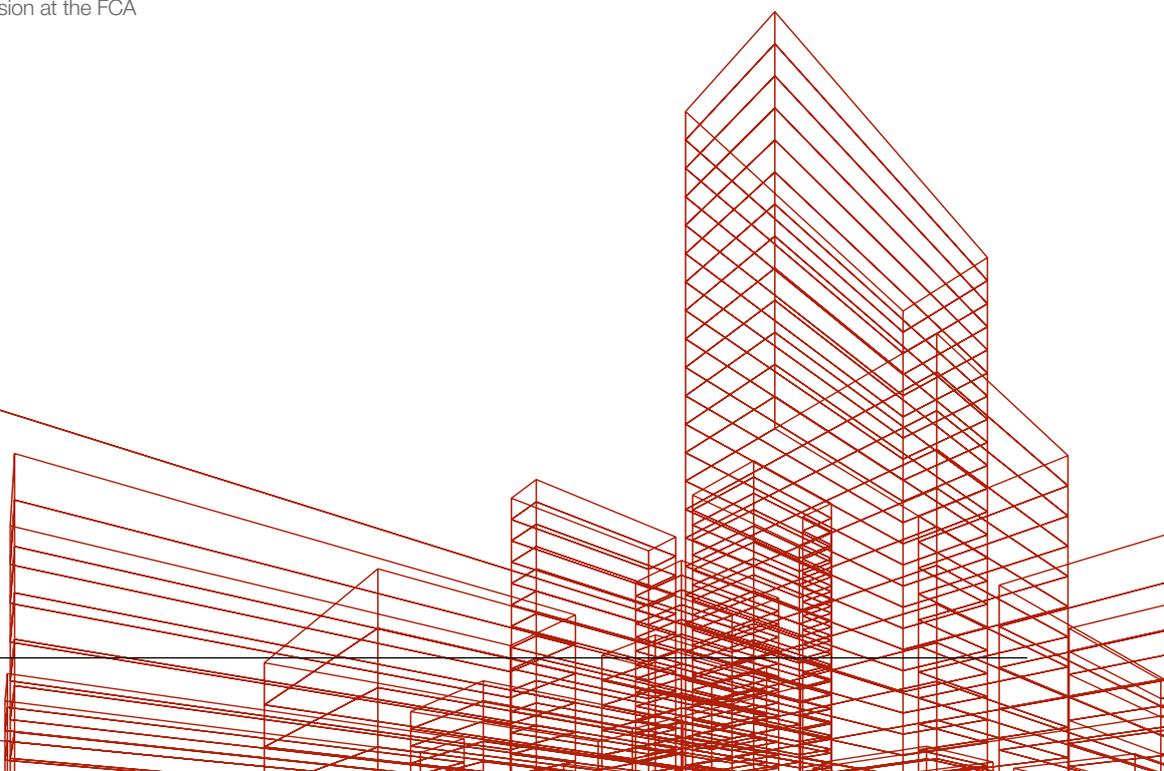
*“The growing pressure to call out inappropriate behaviour in the workplace continues to gather pace”*

At the end of December 2018, Christopher Woolard, director of strategy and competition at the UK's FCA, gave a speech about putting diversity and inclusion on the agenda in financial services. He said: “We have seen a noticeable upturn in reports which concern issues like discrimination and sexual harassment in financial services. Our message to firms is clear: non-financial misconduct is misconduct, plain and simple.”

Megan Butler, the FCA's director of supervision, told the Women & Equalities Committee last year:

*“We do not believe that a culture that tolerates sexual harassment and other forms of behavioural misconduct is a culture that will encourage a safe-to-speak up environment, or an environment where the best business decisions get taken, or where the best risk decisions get taken.”*

Megan Butler, director of supervision at the FCA



## Insolvency risk

Historically, insolvency is the area where directors have tended to be most at risk of claims since, as insolvency approaches, directors' duties move from acting in the best interests of the company to protecting the interests of creditors. While only 32% of our respondents considered the risk of litigation against them as individuals following insolvency or corporate collapse to be a significant concern, almost half identified the current economic climate as a very significant global risk to the organisation's business operations, second only to technological advances.

This concern about economic impact was highest amongst large company respondents and higher still among listed respondents, where 60% felt the economy presented a very or extremely significant risk. UK respondents were the most concerned, and Australians the least, while the sectors that felt most exposed included wholesale, retail and consumer goods; industrial and manufacturing; and services, hotels and leisure.

*“The sectors that felt most exposed included wholesale, retail and consumer goods; industrial and manufacturing; and services, hotels and leisure”*

These fears are not without foundation: In Australia, the total number of companies entering external administration rose to 8,105 for the year 2018-2019, compared to 7,747 for the year before, according to the Australian Securities & Investments Commission. Figures are still down on the 9,800-plus administrations recorded in 2015-16 and 2013-14.

The number of insolvent companies in England and Wales hit a five-year high in the second quarter of 2019, according to data from the government's Insolvency Service. In all, 4,321 companies entered insolvency in the period April to June, the largest total since early 2014. A similar picture of rising corporate insolvencies is also evident across many of the major European economies.

In the UK, 2019 has seen a number of high-profile examples of corporate insolvencies, including those of Thomas Cook, British Steel and a host of restaurant chains and high street retailers. In many of these industries, and particularly on the high street, the challenges for directors have gone far beyond second-guessing the economic climate to include much more fundamental structural changes impacting businesses, such as the move to online shopping.

### A new liability cap for Belgian directors

Running contrary to trends elsewhere, and perhaps motivated by a desire to attract more company headquarters, Belgium this year introduced a cap on directors' liabilities as part of its new Belgian Company Code. The limitation of liability depends on the size of the company and is an aggregate limit that applies to all directors together and is shared between all claimants.

It applies to all liabilities covered by the general directors' liability regime, but does not cover:

- Repeated negligence;
- Gross negligence;
- Intentional fraud; or,
- Liability with the tax and social security authorities.

# Cyber security and data risk

What is abundantly clear from this year's set of survey results is that we have entered a new era of management exposure, with the increasing dominance of cyber attack and data loss now clearly the chief concern for directors and officers. The risks associated with such threats have featured in our survey for many years, but in the last two years have ranked first and second on the list of legal, regulatory and business risks worrying business leaders, overshadowing the growing burden of regulatory and enforcement activity.

This year's survey shows that these threats are becoming more real and concerns are increasingly being realised – in this report, for the first time, more than half of our respondents say they have direct experience of either a significant cyber attack or a sizeable data loss, with the figure rising from 44% last year to 54% in 2019. In 2017, just 24% of interviewees told us that they had experienced such an incident, highlighting the dramatic pace of change in this area.

*“...for the first time, more than half of our respondents say they have direct experience of either a significant cyber attack or a sizeable data loss”*

The exposure to such cyber and data risks continues to be greater the larger the business, with 64% of those working in companies with more than 5,000 employees having been impacted by a cyber event, alongside 55% of listed companies and 60% of multinationals. When we look across geographies, the likelihood of experiencing a cyber attack or significant data loss appears highest in Europe (excluding the UK), where 64% report that they have been impacted, compared to 49% in the UK and 42% in Australia.

The industries that are most exposed include services, hotels and leisure and technology, media and communications, where 66% and 58% respectively report a cyber event significant enough to warrant boardroom attention in the past 12 months. By contrast, the perceived risk of such incidents is lowest in finance, insurance and real estate, according to our survey, with only 42% having direct experience of an event in the past year. This may be due to the heightened awareness and preparedness already in place in those industries.

It is perhaps no surprise that the individuals that we questioned are so alive to the risks associated with data loss, data breach and cyber attack, given the relatively recent advent of the EU's new General Data Protection Regulation (GDPR), which came into effect on 25 May 2018. That law brings with it onerous new obligations, penalties for breaches and a raft of best practice guidelines that few businesses appeared ready for on day one. Its arrival has also coincided with a flurry of high-profile incidents of cyber events at organisations as diverse as a major airline, the European Central Bank and the University of York.

Enforcement action has also been ramping up, with Google receiving a EUR50 million fine from France's information watchdog the CNIL in January 2019 in the first major GDPR infringement case, which centred on failings in the Android set-up process for users creating Google accounts. Other notable actions saw a EUR400,000 fine against a hospital in Portugal for violating GDPR security requirements and an action against the tax authorities in the UK relating to the use of biometric data. Data protection authorities in the UK, Ireland and the United States have all recently indicated that large investigations are in the pipeline and record fines could soon be meted out.

*“Enforcement action has also been ramping up”*

One worrying trend from recent enforcement action by the UK's Information Commissioner's Office is the fact that subsidiaries will be held accountable for compliance failures in parent companies. In one case, Uber's UK companies were fined GBP385,000 in relation to a breach of organisational and technical measures that resulted from a cyber attack on Uber U.S. Uber UK was found to have failed to take reasonable steps to prevent the failure.

Aligned to these concerns is the growing focus by regulators on 'operational resilience', with actions being taken against both firms and senior individuals held accountable for issues such as IT outages. Beyond the issue of protecting against cyber attack comes exposures relating to the use of the wrong hardware or software.

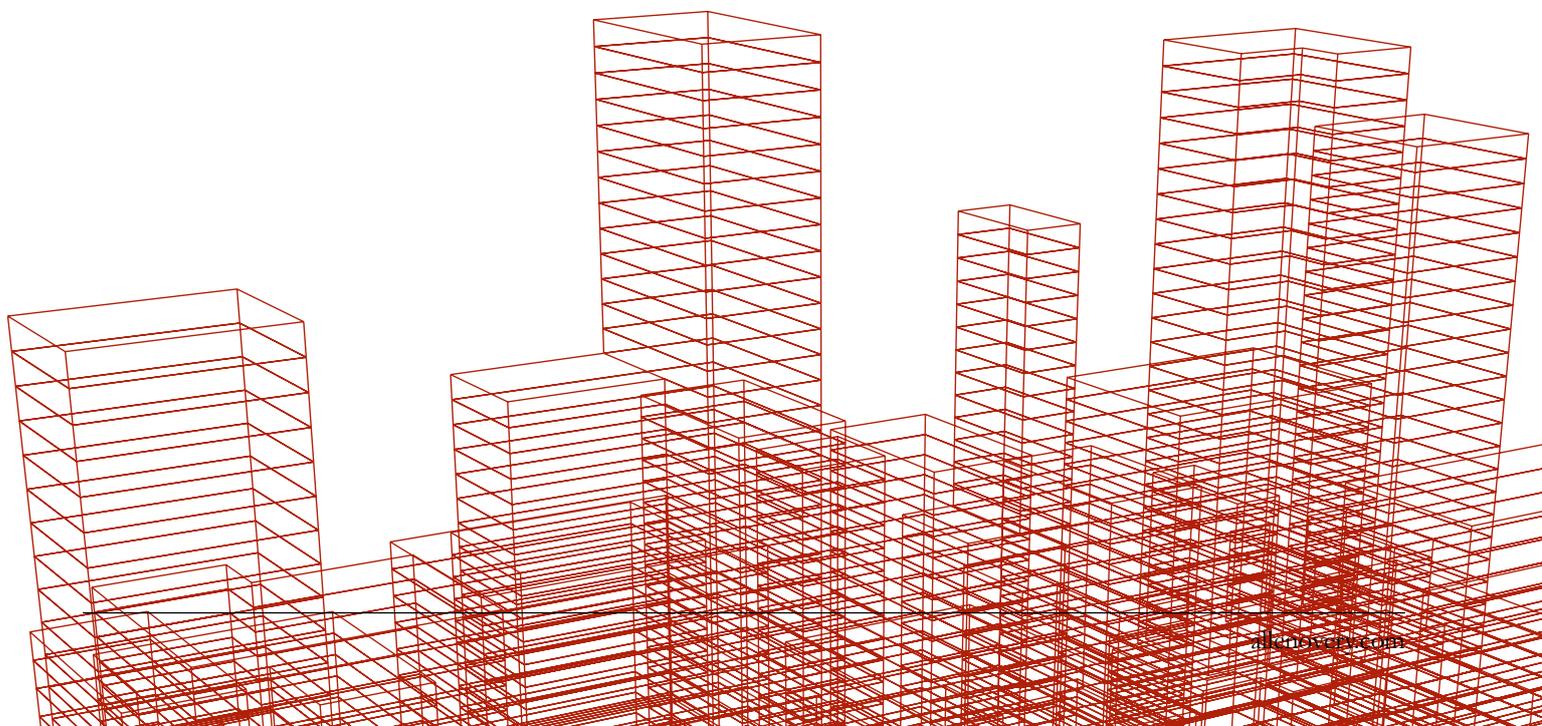
## Data risks

---

Elsewhere, in the financial services sector, where institutions have become accustomed to managing gigantic volumes of data ranging from customer data to business intelligence and employee information, we see the emergence of a new trend towards data ethics. This focuses on the ethical issues relating to data, algorithms and corresponding practices and embodies the difference between what businesses can do with data and what they should do with data, rapidly becoming one of the most significant and complex risk management challenges facing companies.

Senior management are now being asked to look not just at what can be done with data but also what is the right approach morally, which requires the development of data principles and the engagement of stakeholders across the business to ingrain the importance of ethical approaches to data and the implications of getting it wrong.

An additional concern for directors in relation to cyber risk comes in relation to insurance. A recent case involving a large UK supermarket chain saw one of its senior employees deliberately copy the personal data of more than 100,000 employees and then quit the business and upload that data onto a file sharing website. The ex-employee was subsequently prosecuted and jailed for eight years, but some 5,500 of the affected employees then litigated against the supermarket in the English High Court and the company was found vicariously liable for all the criminal actions of the former employee. The Court of Appeal made clear that the availability of adequate and relevant insurance to protect against such liabilities was a relevant factor for directors to consider. That therefore means it may not be long before directors are found negligent for failing to take out adequate insurance to protect a company against cyber risks such as these. This case has come to the Supreme Court on appeal and judgment is awaited.



## Technological risks

Aligned to the concerns associated with cyber security and data protection, where 55% of respondents describe the risks as very or extremely significant, we are also seeing the emergence of technological advances as a new worry for directors and officers. This year, more than half of our respondents (58%) identified risks associated with artificial intelligence (AI) and machine learning as very or extremely significant, and that area was identified as the most significant global risk by companies of all sizes.

In all, 65% of respondents in small businesses, with fewer than 500 employees, were worried about the risks posed to their business operations by technological advances, compared to 55% in large companies. The sectors that showed most concern were wholesale, retail and consumer goods and technology, media and communications.

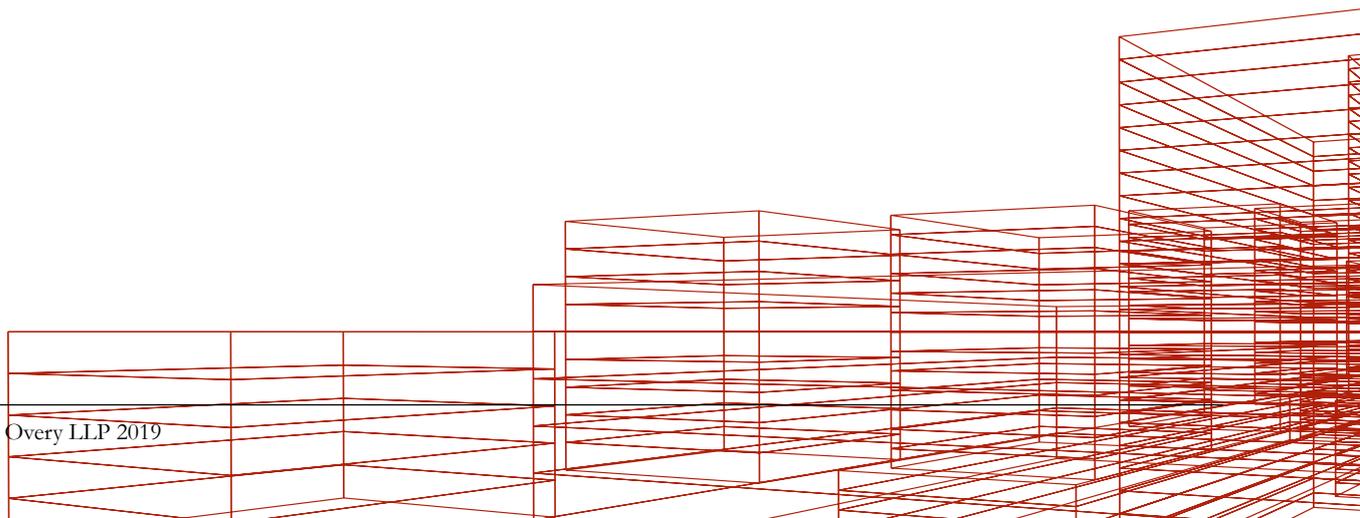
Directors are right to be concerned about the new and emerging risks associated with the use of AI in their businesses, with James Proudman, director of UK Deposit Takers Supervision at the Bank of England, warning financial institutions in June 2019 of the need to keep pace with the speed of change as AI becomes more prevalent. Business leaders may yet find themselves held to account if their company causes harm to others as a result of the unknown and unintended consequences of the deployment of AI, where it is increasingly difficult for directors to keep track of complex algorithms and make sure they are properly supervising the activity taking place in the company's name.

The pace of change is so fast in this area that there may be a need for new skillsets on boards to make sure assessments can be made about the use of machine learning and AI in an informed way. For directors to understand their AI exposures, they need to understand the data inputs that are being used and the way algorithms are reacting to them.

*“The pace of change is so fast in this area that there may be a need for new skillsets on boards”*

The complexity of certain machine learning technologies can create a 'black box' effect, such that it is not always possible to understand how an algorithm has reached a particular outcome. Chess grandmasters are still poring over the strategies deployed by Deepmind's AlphaZero programme to unpick certain (highly successful) moves that were considered to be 'inhuman'. The AlphaZero programme famously taught itself to play chess in a matter of hours, with no human input other than the rules of the game, simply by simulating games against itself.

In practice, this lack of transparency, when allied to any underlying bias in the data being fed to the algorithm, may create unfair outcomes. In turn, this exposes businesses to a range of risks, from reputational damage and loss of goodwill stemming from negative publicity, to loss of revenue stemming from loss of customers. One risk already identified for financial institutions is around unfair or discriminatory decision making, where banks may become exposed to discrimination claims if the algorithm is found to have produced unfair outcomes. There are examples of credit card companies cutting credit limits when charges appeared for marriage guidance, for example, because marriage breakdown is often linked to debt default. Likewise, algorithms can generate gender bias if left to make their own decisions on insurance premiums and algorithmic trading can create still further exposures. The skills gap at board level, taken together with the supervisory responsibility of directors, explains why such concerns are increasingly keeping leaders awake at night.



The potential lack of transparency is part of a broader issue inherent in AI and machine learning technologies: AI ethics. In practice, AI ethics embodies the difference between what businesses can do with AI, and what they should do with AI. Many of the existing legal standards applicable to AI technologies are not fit for purpose. For instance, there is a fundamental tension between the core principles of data protection law in the EU (and in many other jurisdictions) – such as transparency and accountability – and a technology that relies on access to vast datasets to perform complex calculations well beyond human capability. For this reason, many businesses are considering the appropriate ‘compliance-plus’ standard for their AI programme, which takes into account how public opinion might perceive actions if those actions were to be made public.

*“Many of the existing legal standards applicable to AI technologies are not fit for purpose”*

Indeed, AI ethics is rapidly becoming one of the most important strategic and, given its philosophical heritage, operationally complex risk management challenges facing companies. If a company is perceived to be using data in an underhand or reckless way, it could face significant consequences, including loss of customer trust, regulatory investigation and investor backlash.

There are many different ways of thinking about ethics and what is ‘ethical’ will mean different things to different people. A company’s directors will be responsible for establishing the appropriate parameters for their use of AI technologies. There are likely to be geographical divergences on approach. For instance, there is a philosophical difference between the approach to data protection in China, where the state guards the data, and the EU, where the state is guarded from the data.

Regulators are also focusing on ethics as the means by which AI technologies are, and will likely in the future be, regulated. Between them, regulators around the world have produced no fewer than 84 (and counting) codes of ethics for AI. These are generally very high level, enshrining principles such as fairness, prevention of harm, explicability and safety. Directors of businesses operating in multiple jurisdictions will need to consider any divergences between the regulatory approaches to AI technology.

*“Regulators around the world have produced no fewer than 84 (and counting) codes of ethics for AI”*

These factors have led to data ethics – and AI more generally – being an issue that directors cannot afford to ignore. Translating ethical principles into practice, and mitigating the risks posed by AI without impairing the benefits, are challenges for almost every business. Directors are in a position to ensure that appropriate practices and procedures are embedded in relevant parts of the business.

# Protecting directors and officers

## Insurance market conditions

---

Given the ever-growing list of personal liabilities that directors now find themselves exposed to, the attention being paid to the availability of D&O insurance and the related question of indemnities shows signs of continued growth. Several London market realities are impacting the D&O insurance market and the trend towards a hardening, driven in part by increased claims activity, was identified in our last report and has since accelerated. Today, market conditions for D&O are as challenging as they have been for many years.

Whilst overall capacity in the global market is still theoretically in excess of USD1 billion, we are witnessing a significant reduction in appetite such that insurers are often reducing their participation on a particular risk.

We are also seeing the imposition of more restrictive conditions and a generally less flexible approach to amending coverage terms. Insurers are increasingly using sub-limits and tailored exclusions and/or higher deductibles to curb their exposure to what they perceive to be high risk areas. Finally, premium rates are subject to significant increases across virtually all sectors and industries, including those which have previously enjoyed benign and stable prices over many years.

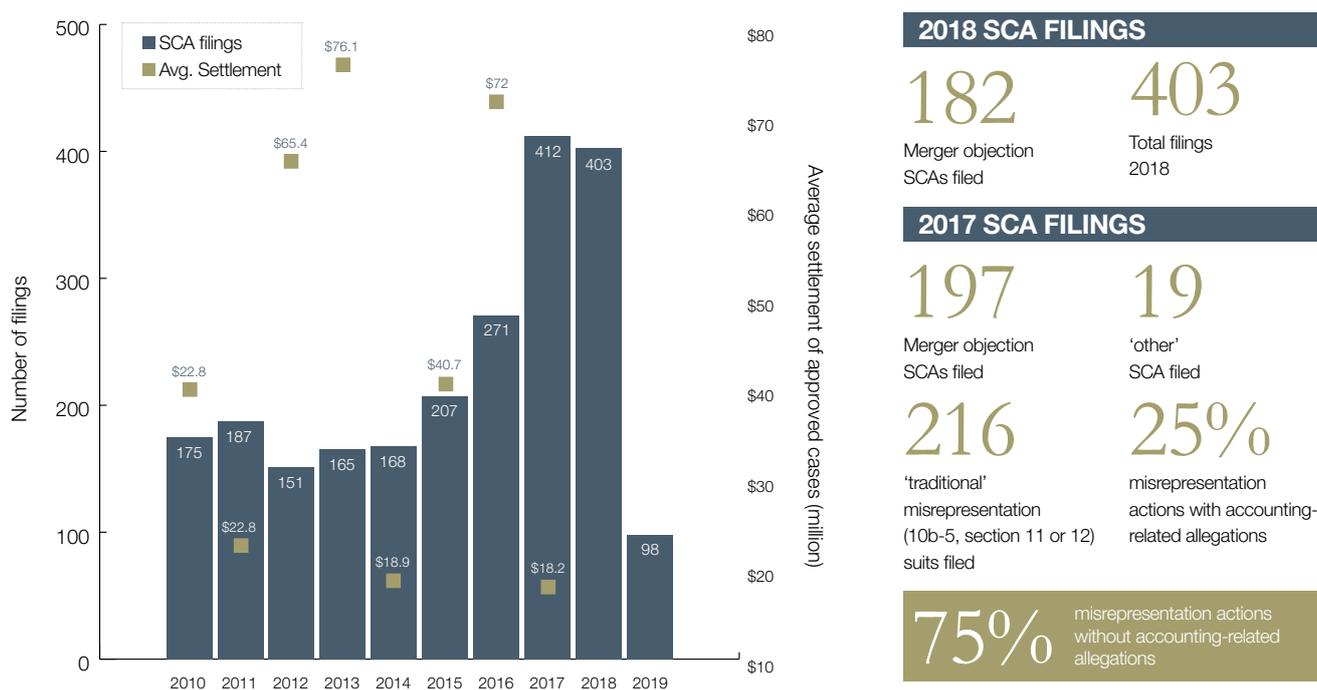
We are witnessing significant reductions in 'usable' capacity, especially in relation to companies with large U.S. securities exposure where typical capacity may now be as little as USD5m per insurer.

There are a variety of reasons behind this marked and continuing deterioration in market conditions but there is little doubt that claims, both new and historic, are a major factor. D&O insurance is typically labelled as 'long tail' business, as it can be not until many years after a claim has been notified to insurers for attachment purposes that defence costs start to be incurred in earnest as litigation ramps up. Indeed, some of the large claims notified after the 2008 financial crisis fall into this category and have yet to be concluded.

On top of this, new U.S. securities class action filings continue to grow at almost unprecedented levels and show no signs of slowing down, as the table on the following page shows.

## Directors and officers liability

### Federal securities class action filings and average settlement at Q1 2019



### 2017 SETTLEMENTS

	Less than USD10m	USD10-19.9m	USD20-49.9m	USD50-99.9m	USD100m or greater
2017	61%	11%	14%	7%	8%
2018	51%	13%	17%	5%	15%
2019	58%	13%	9%	7%	13%

The trend towards event-based case theories, used both by plaintiffs' lawyers in the U.S. and by an increasingly sophisticated international plaintiffs' bar, has also led to an increase in litigation risk. A typical event-based case theory posits that virtually any manner of serious incident or outcome affecting a company's fortunes could or should have been anticipated by the company's management. Nevertheless, and despite this, appropriate preventive measures were not taken which, if they had been taken, would have either prevented or significantly mitigated the damage, meaning that the directors should be held liable. Whilst the track record for this case theory may be patchy at best, defence costs associated with rebutting these claims can be considerable.

Finally, the regulatory focus on personal accountability at board level that we have highlighted so often in the past shows no sign of

abating. Investigations into both firms and individuals, especially in the regulated sectors, are running at almost unprecedented levels. Recent data from the FCA shows it was investigating 58 directors as of December 2018, more than double the 24 identifiable targets in 2016 when the new SM&CR came into force.

Regulatory investigations can and often do drag on for many years and cost insurers a lot of money in legal representation expenses for the directors and other executives involved. This continues to add fuel to the overall loss experience of insurers in this sector. Where investigations result in sanction or criticism of firms or entities, these are often later used by civil claimants to bolster their claims, augmenting the circle of loss.

## Policy priorities

Every year as part of this survey, we ask respondents about their priorities when it comes to securing D&O cover. This year there is an interesting and direct correlation between many of the forces giving rise to the hardening market referred to above and the biggest concerns affecting individual directors. For the first time, the top threshold coverage issue is how claims against directors and officers will be controlled and settled. Just three years ago this was only the fifth priority and before that it did not even feature as a worry. In a sense this earlier absence is strange since, after all, the claims process ultimately determines where the policy will pay out. One explanation may be that now, for the first time, directors are appreciating the importance of ensuring not just that they have a policy in place whose terms are clear and easy to follow, but that it is indeed fit for purpose in an increasingly hostile claims environment.

Related to the top concern is the next biggest worry for directors, which is how they can access, and/or control access to, the policy. Perhaps what underlies this is a deeper concern as to whether there will always be sufficient limits left to pay all defence costs and other liabilities for the whole class of insured persons. Bearing in mind that most policies operate on a shared aggregate or single pot basis, and that in a large company hundreds or even thousands of employees might be eligible for cover, this makes sense.

Under English law, the general principle governing the order in which insurers pay out the policy limits is first-come, first-served. If you are a non-executive director considering the adequacy of the limits purchased you may have a particular concern here, given that the standard approach to regulatory investigations is bottom up, ie investigators will start with more junior executives and work their way up towards the board. This means that perhaps meaningful parts of the cover may be eroded before the board is able to access it.

### There are some other interesting findings when one digs more deeply into the responses

- We asked how important to directors is the question of what happens to the cover when the company goes insolvent. There are stark differences in the responses depending on industry sector. In the services, hotel and leisure sectors, for example, 69% regard this as extremely or very important, as do 68% of industrial and manufacturing companies. By contrast, only 34% have similar concerns in government and public services sector and 53% in finance, insurance and real estate industries. To some extent these numbers may be a proxy for more general concerns about financial strain in the various sectors.
- There is a perhaps correlated set of variances in response to the question of the importance of competitive pricing, with only 34% concerned about this in government and public

services sector as against 47% in finance and insurance and real estate industries and 64% in industrial and manufacturing companies. Overall, the significant hikes in premium rates referred to above have also had an effect. Whereas in 2017 a record low of only 15% were concerned about this issue, by 2019 the equivalent number has risen to 55%.

- We also asked how important it is to directors that they understand how coverage disputes with insurers will be resolved. Among respondents in Australia, 73% regard this as very or extremely important, whereas in Europe (excluding the UK) this percentage falls to 51% and in the UK it stands at 62%. Again, a cautious but perhaps legitimate interpretation of these differences might attribute them to a variance in the perceived risk of such disputes arising in the first place.

## The clawback issue

Anecdotally, we have noted a rise in questions and concerns from directors on the practical question of what happens in cases where perhaps significant sums are advanced by insurers for defence costs under a reservation of rights. A typical scenario might be that allegations of fraud or dishonesty are levelled against insured persons in underlying litigation. D&O policies invariably contain dishonesty and fraud exclusions. However, almost all such policies will also provide for the advancement of defence costs in this situation until there has been some kind of final adjudication or formal admission by the directors with respect to the alleged conduct.

This advancement will usually be accompanied by a communication from insurers to the effect that, in the event there is a finding of fraud or dishonesty, the insurers reserve the right to ‘claw back’ the money. How does this work? First, we need to distinguish between those policies that expressly provide insurers with a contractual clawback right in these circumstances. Here there is little doubt but that insurers can require the directors to repay. Other policies are silent on the issue, so the question is more nuanced. Is the commitment to ‘advance’ defence costs, albeit under a reservation of rights, legally different to the obligation to ‘pay’ such costs once and for all? Much will depend on the precise language used.

Having said all that, our experience as a practical matter is that insurers rarely if ever seek to exercise their contractual clawback rights. In most cases they conclude that there is little point in throwing good money after bad in circumstances where the directors concerned may struggle to find the funds. One potential sting in tail to watch out for here, however, is a provision that permits insurers to recover defence costs by way of clawback not just against the insured who has benefitted but from any insured, including the company.

Of particular interest on this point will be how the cover advanced under the D&O policy will be dealt with in the event the company negotiates a deferred prosecution agreement (DPA). The question as to whether a DPA amounts to a final adjudication under D&O policies remains unclear and the only safe course for a company or individual when considering embarking upon negotiations to enter into a DPA is to work closely with insurers so that the indemnity implications of doing so are fully understood.



*“When a claim happens the directors and officers who are in the firing line depend heavily on the D&O cover for their peace of mind. In particular, they need to understand with absolute clarity what the D&O cover provides. High on their priorities is whether there is a risk of insurers seeking to clawback defence costs if things do go wrong.”*

Eve Giles, Partner – London

# A guide: practical tips on D&O and indemnities

## Indemnification and insurance products: understanding the gaps

The two key protection products available to senior managers and directors are D&O insurance and indemnities. There are legal restrictions governing what businesses can indemnify their directors and officers against, but both D&O policies and indemnities can be complex and, of course, their exact details will vary by underwriter.

With more than one way of getting protection, directors need to be mindful of how their D&O policy coordinates with their company's indemnification obligations. There are important lessons to draw from the gaps that exist between these two protection products, as the table below shows.

Gaps in a D&O insurance policy	Gaps in a company indemnity contract
<p>Applies to Directors and Officers only, subject to policy wording.</p>	<p>Applies to all employees and officers of a company who are not also directors (or statutory auditors).</p>
<p>D&amp;O is designed to respond to liability for claims (including defence costs) made and investigations commenced against directors in a particular period of insurance. As such it provides limited, if any, protection in the absence of a claim or investigation directly involving the individual concerned.</p> <p>Cover is often complex and comes with built in restrictions and exclusions.</p>	<p>An individual has no automatic right to indemnity. Such rights to indemnity as he or she may have, may be further limited by:</p> <ul style="list-style-type: none"> <li>– statutory restrictions</li> <li>– the terms of any relevant contract (or deed poll)</li> <li>– the company's willingness and appetite to indemnify based on:                             <ul style="list-style-type: none"> <li>– its perception of the facts on the ground in each case, and</li> <li>– whether the senior manager is still in post when the indemnity is called upon.</li> </ul> </li> </ul>
<p>The insurance limits themselves are usually shared between a large group of individuals which is not restricted to senior executives (and often includes the company itself).</p> <p>Hence the limits are prone to rapid depletion and even exhaustion.</p>	<p>The company indemnity will be worthless in the event of company insolvency.</p> <p>The indemnity may not continue after the individual has ceased to be employed. Even if it does, the terms may not be as generous.</p>

The most common trigger for a covered insurance claim is an allegation made against an individual that he or she has committed a wrongful act in a management or executive capacity. Whilst it is dangerous to generalise, most good D&O policies will also provide protection to directors who are either the target of a regulatory investigation or who are required to attend an interview in the context of such an investigation.

## What can executives do?

---

Senior managers and directors can and should prepare for the new regulatory focus on their individual conduct. A useful starting point would be to take responsibility for clarifying one's own

responsibilities and reporting lines, as well as understanding the detail of the personal liability protection available through D&O insurance or employer's indemnity.

To help, below is a checklist that covers the most important questions that senior individuals may wish to consider with their employers.

---

- 1 With which categories of employee, at what level of seniority, do I share the D&O limit purchased by the company on my behalf?
- 2 Is my D&O limit also shared with the company itself and, if so, in what respects and to what extent?
- 3 Is access to my D&O insurance policy dependent on a failure or refusal by the company to indemnify me?
- 4 Does the company agree to indemnify me in respect of all legal expenses (including, where I consider it necessary, seeking independent legal advice) in my capacity as a senior manager, to the extent legally permissible?
- 5 In pre-enforcement dealings with regulators, what cover (if any) is available to me to seek independent legal advice under the employer's D&O insurance programme?
- 6 Will there be cover for internal investigations?
- 7 Will there be cover for travel expenses for meetings with regulators (both in the directors' home country and abroad)?
- 8 Is the indemnity wide enough to cover all board appointments (including appointments to clients, any joint ventures or subsidiaries which are not wholly owned)?
- 9 If the answer to 4 and/or 5 above is 'No/None', has the company considered purchasing additional legal expenses for me in pre-enforcement dealings with regulators?
- 10 What restrictions are imposed (both by indemnity and insurance) on my freedom to select lawyers of my choice and in the conduct and control of my defence?
- 11 Does the policy provide a mechanism under which insurers will advance all defence costs and legal representation expenses to me, pending resolution of any dispute between the company and the insurers as to the extent of such costs ultimately covered under the policy?
- 12 What protection do I have against future claims against me if I retire or resign during the policy period, or if during such period the company is the subject or object of mergers and acquisitions activity?
- 13 Does my D&O policy contain provision to enable me to take proceedings to clear my name in appropriate cases?

## *A company indemnity vs. a D&O insurance policy – what can they do for you?*

### What only a D&O insurance policy can do for you

---

Only a D&O insurance policy can provide protection in the form of:

- defence costs cover (civil, regulatory and criminal proceedings), with no repayment risk in the event of the director being found to have acted wrongfully unless they are found to have acted dishonestly or fraudulently;
- cover for director/officer liability to the company or an associated company. The law precludes a company from providing a director with indemnity protection in respect of liability to the company itself, so a D&O insurance policy can provide a broader range of indemnity protection than a company indemnity can do;

- a source of indemnity protection that is independent of the company, thus removing the conflict problems that arise when the company is involved in the claim against the director; and
- a source of indemnity that is available even if the company has become insolvent (rendering any corporate indemnity valueless).

But a D&O insurance policy will be subject to policy exclusions and an aggregate policy limit that does not appear in typical indemnity arrangements, and a D&O policy is subject to an annual renewal and renegotiation process.

### What only an indemnity contract with the company can do for you

---

Only an indemnity agreement can, subject to its terms, provide protection in the form of:

- an uncapped indemnity;
- no policy exclusions (though most indemnities do include a number of conditions);
- no insurer payment refusal/default/insolvency risk; and
- a long-term indemnity assurance, which is not subject to annual renegotiation, and thus to the risk of change or cancellation.

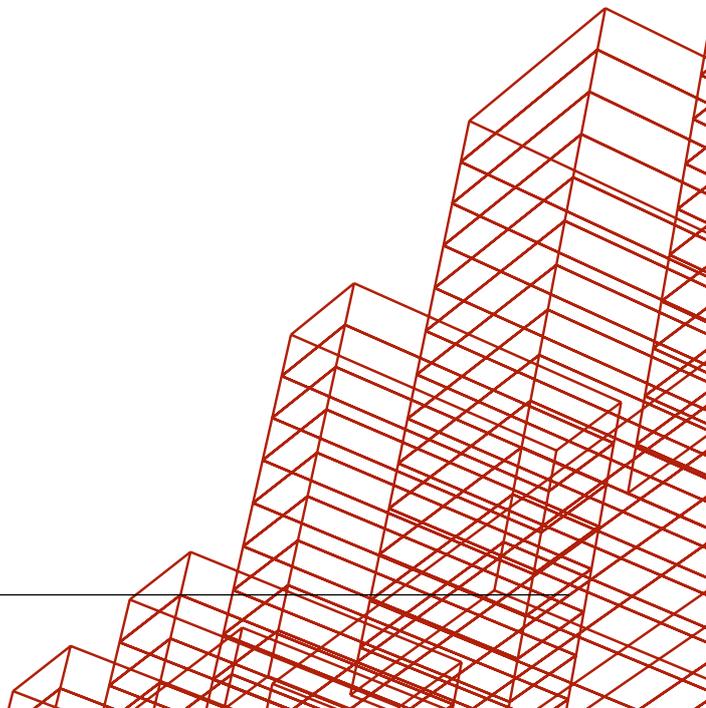
But restrictions imposed by law on the scope of what is permitted by way of indemnification to a director mean that an indemnity contract for a director is likely to be more limited in its scope, and that defence costs are only available as incurred on the basis of a loan, which could potentially have to be repaid if the director's defence fails.

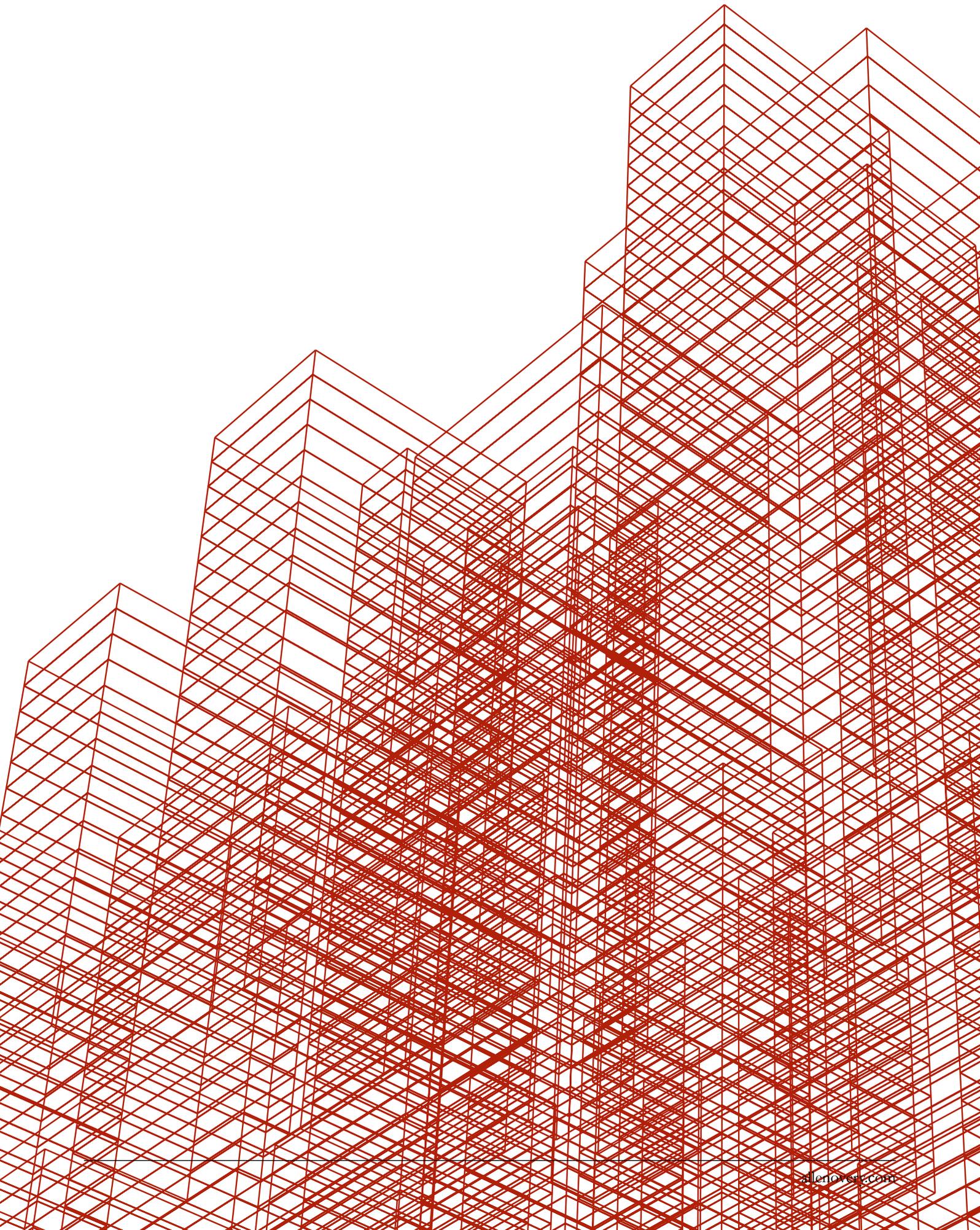
### What neither D&O insurance nor company indemnity can do for you

---

Neither a D&O insurance policy nor a corporate indemnity will provide a director or officer with indemnity protection against:

- liability arising by reason of the director's dishonest, fraudulent or criminal conduct; or
- criminal fines or regulatory penalties.





---

## GLOBAL PRESENCE

---

Allen & Overy is an international legal practice with approximately 5,400 people, including some 550 partners, working in over 40 offices worldwide. Allen & Overy LLP or an affiliated undertaking has an office in each of:

Abu Dhabi	Bucharest (associated office)	Hong Kong	Munich	Singapore
Amsterdam	Budapest	Istanbul	New York	Sydney
Antwerp	Casablanca	Jakarta (associated office)	Paris	Tokyo
Bangkok	Dubai	Johannesburg	Perth	Warsaw
Barcelona	Düsseldorf	London	Prague	Washington, D.C.
Beijing	Frankfurt	Luxembourg	Rome	Yangon
Belfast	Hamburg	Madrid	São Paulo	
Bratislava	Hanoi	Milan	Seoul	
Brussels	Ho Chi Minh City	Moscow	Shanghai	

**Allen & Overy** means Allen & Overy LLP and/or its affiliated undertakings. Allen & Overy LLP is a limited liability partnership registered in England and Wales with registered number OC306763. Allen & Overy (Holdings) Limited is a limited company registered in England and Wales with registered number 07462870. Allen & Overy LLP and Allen & Overy (Holdings) Limited are authorised and regulated by the Solicitors Regulation Authority of England and Wales.

The term **partner** is used to refer to a member of Allen & Overy LLP or a director of Allen & Overy (Holdings) Limited or, in either case, an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings. A list of the members of Allen & Overy LLP and of the non-members who are designated as partners, and a list of the directors of Allen & Overy (Holdings) Limited, is open to inspection at our registered office at One Bishops Square, London E1 6AD.

© Allen & Overy LLP 2019. This document is for general guidance only and does not constitute definitive advice.

UK  
CS1911\_CDD-57482\_ADD-87058