ALLEN & OVERY

Willis Towers Watson

Directors' liability

D&O: Personal Exposure to Global Risk

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

November 2018

Contents

Introduction

At a time when regulators and investigatory authorities are focusing unprecedented attention on personal accountability for company directors, we are pleased to bring you the sixth edition of our series on directors' liabilities. A joint effort by international law firm Allen & Overy LLP and the global risk management brokerage and advisory firm Willis Towers Watson, we began this exercise to investigate boardroom attitudes to risk back in 2011 when, in the immediate aftermath of the global financial crisis, directors and officers began to find themselves in the spotlight as never before.

For the first time this year we see our respondents' concerns dominated by the threats of cyber attack and data loss – fears that are not new but are rapidly moving up the agenda. In this year's survey, 44% of respondents tell us they have experienced a significant cyber attack or data loss in the past 12 months, which is nearly double the 24% that had been on the receiving end of such an issue when we asked the same question a year ago. The advent of the EU's General Data Protection Regulation, which came into effect in May 2018 as the most significant change in data privacy regulation in decades, has only added another layer of complexity to an already challenging cyber environment.

This year we have surveyed 161 directors, non-executive directors, partners, in-house lawyers, risk officers and compliance professionals, working all over the world. Their responses paint a picture of heightened anxiety and exposure. This is unsurprising. Seven years on from the first survey in 2011 and conditions have become noticeably more challenging, with high-ranking individuals in public and privately-held corporations facing unprecedented scrutiny and bearing the brunt of global enforcement efforts to combat corporate failings. As you will see on the following pages, the threat of civil and criminal claims is a growing concern, as governments, legislators and regulators around the world work to improve business cultures by concentrating on the behaviours of those in positions of power. Particularly noteworthy is the aggressive stance of the Serious Fraud Office: the number of Section 2 notices issued by the SFO has jumped by 41% in the last year alone, from 730 cases in 2016/2017 to 1,032 cases in 2017/2018.

We have called this year's report Personal Exposure to Global Risk, because we continue to see the spotlight on individuals chiming with a much broader extraterritorial remit for those tasked with enforcement. Today's respondents are likely to have experienced a regulatory claim involving a director in their business, and that focus on personal accountability is having an impact on the way in which they run their businesses, with 60% reporting a change to the way decisions are made, and half identifying a change in the company's appetite for risk.

For the first time, health and safety is regarded as a top-five concern for directors. Given the Grenfell Tower fire in the summer of last year, and the Genoa bridge collapse in August 2018, a surge of concern in relation to these kinds of issues is perhaps foreseeable. Anxiety over employment claims is also on the up, maybe as a result of the #metoo movement.

When it comes to D&O protection, our interviewees highlight the importance of insurance that will be able to respond to claims in all jurisdictions, which has moved up the list of priorities significantly compared to previous years. Also rising up the agenda is a broad definition of who is insured, which had not previously featured in the top five, while clear and easy to follow policy terms are no longer the top issue, dropping to fourth having consistently topped our findings since 2013.

We hope you find our coverage and analysis useful. Should you require any further information on any of the issues raised here, please do not hesitate to get in touch with your usual contact at either Allen & Overy LLP or Willis Towers Watson.

Joanna Page
Partner, Allen & Overy
joanna.page@allenovery.com

Francis Kean
Executive Director,
Willis Towers Watson
francis.kean@willistowerswatson.com

Executive summary

51% of public companies experienced a cyber attack or data loss last year, up considerably on the 30% that did so in 2017.

For the first time, **cyber attack and data loss/breach tops the list of risks directors are most concerned about**, overtaking regulatory and other investigations.

43% of large employers have experienced a regulatory claim involving a director in the last 12 months, and 38% of listed companies.

The **regulatory focus on personal accountability is changing company behaviour**, with 60% saying it is impacting decision-making processes.

75% of UK respondents point to growing economic and geopolitical risks impacting their firms, compared to just **47% of respondents in non-UK companies.**

Health and safety legislation impacting on a company's business is now a significant concern for **37%** of respondents, as against just **18%** of those surveyed last year.

When we look at policy terms, the biggest concern for the first time ever is **whether a D&O policy will be able to respond to claims in all jurisdictions**.

Personal exposure to global risk – our key findings

Top five risks to businesses, year-on-year

Top five policy coverage issues, year-on-year

International exposure in uncertain times

Ever since we published our first report looking at boardroom risk and the D&O markets in 2011, we have been using this research as an opportunity to analyse the state of directors' liabilities in the UK and abroad. Over the years we have considered in depth how regulators and policymakers around the world have redoubled their efforts to influence corporate cultures and behaviours by increasing the personal accountability of those in charge, and we have borne witness to the work being done by enforcement agencies to prioritise individual responsibility in the face of corporate wrongdoing.

But the nature of risk continues to evolve and this year, in addition to regulatory risk and the huge new challenges presented by cybercrime, we find significant additional risk to businesses is being created by the global economic climate. Some 68% of our respondents reported that current economic conditions are creating a new level of risk, while two-thirds also pointed to challenges created by geopolitical uncertainties.

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

According to the World Economic Forum's Global Risks 2018 report, the escalation of geopolitical risks was one of the most pronounced trends of 2017, particularly in Asia, where the North Korea crisis arguably brought the world closer than it has been for decades to the possible use of nuclear weapons. That report points to challenges being created around the world by rising inequality and unfairness, the risk of conflict, environmental and extreme weather challenges, and a decline in commitment to rules-based multilateralism.

These macroeconomic and political risks were of biggest concern to the leaders of mid-tier companies, employing between 500 and 5,000 employees, where more than 70% expressed worries, compared to a figure of 57% for those in smaller businesses. But whether respondents have in mind the uncertainties associated with Brexit negotiations in the UK, trade wars between the United States and China, conflict in the Middle East or tensions between Russia and the West, the percentage of respondents who worried about the geopolitical environment did not fall below 67% for any world region in our survey and was highest in Europe and North America.

There was a big discrepancy between the views of those working in UK companies and those in the rest of the world, with 75% of UK company respondents pointing to significant additional risk from economic and geopolitical conditions, compared to 47% for respondents working in companies headquartered elsewhere. This perhaps points convincingly towards Brexit-related anxiety.

For business leaders, this climate heightens the risks associated with operating internationally, and our respondents point to several significant risks in this context: the difficulties of dealing with multiple sanctions regimes; the risks of company directors being sued abroad; and the risks associated with key employees being extradited by foreign governments.

Also of growing concern is the ability to protect the reputation of both businesses and individual directors in the face of intense scrutiny. Risks associated with health and safety, climate change, human rights and community impact are moving up the agenda in this context.

The percentage of respondents who worried about the geopolitical environment did not fall below 67% for any world region in our survey and was highest in Europe and North America.

Health and safety

For the first time, health and safety as a risk category has made it into the top five anxieties for directors. Health and safety can cover a wide range of issues for different directors and has been bubbling below the top five concerns for a while. Anecdotally, we know from clients that such issues are a major concern for directors who are keen to ensure that the products that their companies provide, or the workplaces in which their employees operate and members of the public visit, are entirely safe.

Failure to provide such safety can lead in almost every jurisdiction to fines for the company and, very occasionally, for directors themselves if they are directly part of the systems failure that has led to an accident. This does not of itself explain the heightened concern in this year's survey, which may be partly a result of concern around climate change and the accelerating importance of human rights and corporate social responsibility in the business environment.

In the UK, figures published by the Health and Safety Executive on the total amount of fines imposed annually are calculated to the end of March, so 2017/18 figures are not yet available. However, total fines for the year 2016/17 were GBP69.9m, up from GBP40m the previous year as new sentencing guidelines came into effect. Fines are now related to the turnover of organisations and, as a result, large organisations convicted of offences are receiving larger fines than in the past. In the 2016/17 period the single largest fine was GBP5m and a total of 38 cases received fines over GBP500,000.

The threat of corporate manslaughter prosecutions in the wake of several high-profile infrastructure tragedies must also weigh heavy on the minds of company directors. Following the fire at Grenfell Tower in London in June 2017, senior executives from the council and the tenant management organisation have been investigated by police, while in Italy, prosecutors are investigating managers of the company responsible for the motorway bridge that collapsed in Genoa in August 2018.

Following the fire at Grenfell Tower in London in June 2017, senior executives from the council and the tenant management organisation have been investigated by police, while in Italy, prosecutors are investigating managers of the company responsible for the motorway bridge that collapsed in Genoa in August 2018.

Climate change

On the subject of climate change, a federal judge in New York this year threw out a case brought by New York City against five major oil companies for their role in contributing to climate change, where it was argued that the companies should compensate the city for the cost of mitigating the effects of global warming. New York is one of several cities that has filed similar suits, and it looks likely that cases involving environmental impacts of company operations will become more common.

There is a growing concern that claims will proliferate, exposing not merely the corporate entities but also individual directors to personal criticism (see the Sabin Centre for Climate Change Law, which tracks climate change litigation). Some say that it will be the new wave of litigation, akin to the tobacco litigation of earlier decades, and that there will be a focus on those companies that pushed forward with new energy projects in the face of awareness of an increased risk of climate change.

There is also increasing readiness in the developing world to seek redress for damage. In most jurisdictions individual directors will not face personal exposure for such claims, but directors are concerned, particularly in a world driven by social media, as to whether their personal reputations will be on the line.

Human rights and community impact

Likewise, we can expect to see more enforcement in the area of human rights and community impact. Allen & Overy LLP recently published the fifth edition of the Business and Human Rights Review, in which it highlighted the French 'corporate duty of vigilance' introduced last year, which imposes on large French corporates a duty to detect and prevent the risks of serious violations of human rights, fundamental freedoms and of environmental damage in France and abroad.

The trend towards increased regulation and scrutiny of companies' human rights impacts continues across the world, with the court of public opinion – which also sets out its case in 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.

For example, the collapse of the garment factory Rana Plaza in Dhaka, when over 1,000 people died and many more were injured, has led to much greater focus on supply change responsibility and the reputational risk generated across the supply chain. Whilst the entities that may have contracted products from the site may legitimately claim they have no legal responsibility for the work conditions under which companies operated several rungs below in the supply chain, the tragedy that unfolded made shocking headlines around the world and caused substantial reputational harm to many of the companies involved.

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. Figures from the UK Crown Prosecution Service show that in the year 2017-18, 239 suspects were charged with modern slavery offences, and 185 people were convicted, with prosecutions up by a quarter on the previous year.

Breaches of human rights will also increasingly lead to a risk of prosecution – see the recent changes to the Proceeds of Crime Act 2002 to provide for recovery of the proceeds of gross human rights abuse or violation.

Sanctions regimes

Turning to international risks, Russia has become 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 the sanctions target individuals, major Russian state banks and a list of corporations, while restricting access to EU and 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.

More recently, in November 2018, the U.S. imposed sanctions on 700 Iranian targets (focusing on the oil, financial and shipping sectors) – the U.S.'s largest ever single-day action targeting Iran, which aims to disrupt Iran's regime.

In the UK, the new 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 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.

Foreign Corrupt Practices Act and the UK Bribery Act

It was the advent of America's Foreign Corrupt Practices Act (FCPA), and the UK Bribery Act, that highlighted the extraterritorial exposures of directors and officers operating internationally. Both Acts apply to foreign firms and persons who cause, directly or indirectly through the actions of agents, a corrupt payment to take place on U.S. or UK soil, and relate to foreign corruption if some or all of the facilitation happens in the UK or the U.S., or if foreign firms conduct business in the UK or the U.S.

During the second quarter of 2018 alone, there were five corporate FCPA enforcement actions, with companies paying a total of USD985m in fines between them. Chief amongst them was the fine against Société Générale – the first coordinated enforcement action by the U.S. Department of Justice and the French authorities in an overseas corruption case. SocGen paid USD585m to resolve Libya FCPA offences, with half of the FCPA penalty payable to the French enforcement agency Parquet National Financier.

Law enforcement agencies are collaborating more effectively than ever before to secure the prosecution of anyone involved in wrongdoing, and an individual found guilty of a breach of the FCPA or the UK Bribery Act can be fined, debarred from holding office in future, or imprisoned. In 2017, there were 20 individual FCPA enforcement actions, many involving presidents, CEOs and COOs who either authorised corrupt payments or turned a blind eye.

EY published the 12th edition of its UK Bribery Digest in March 2018, which focuses on commercial bribery cases and showed six cases reported in the preceding six months, bringing the total to 77 in the past decade. Four of those six most recent cases had corporate data at their heart, while another involved a classic overseas bribe to win a contract.

Law enforcement agencies are collaborating more effectively than ever before to secure the prosecution of anyone involved in wrongdoing.

The plaintiffs' bar

Another new topic of concern to the majority of our respondents is the possibility of class action lawsuits against a company and its directors. Most of the individuals surveyed are aware of the existence and growth of a plaintiffs' bar outside the U.S., by which we mean law firms focused on coordinating and representing groups of individuals in class-action litigation in other parts of the world. This development is something that 55% see as a moderate or great threat to themselves or their businesses.

Spurring the growth of the plaintiffs' bar in the UK has been the arrival of third-party litigation funders, capable of putting together sizeable war chests to support the financing of claims, in return for a percentage of awards. In particular, the success of a group of RBS shareholders in pursuing claims against the bank and its bosses over a GBP12bn cash call in 2008, which was backed by third-party funding, is likely to set a precedent for more claims against business leaders being pursued through the courts.

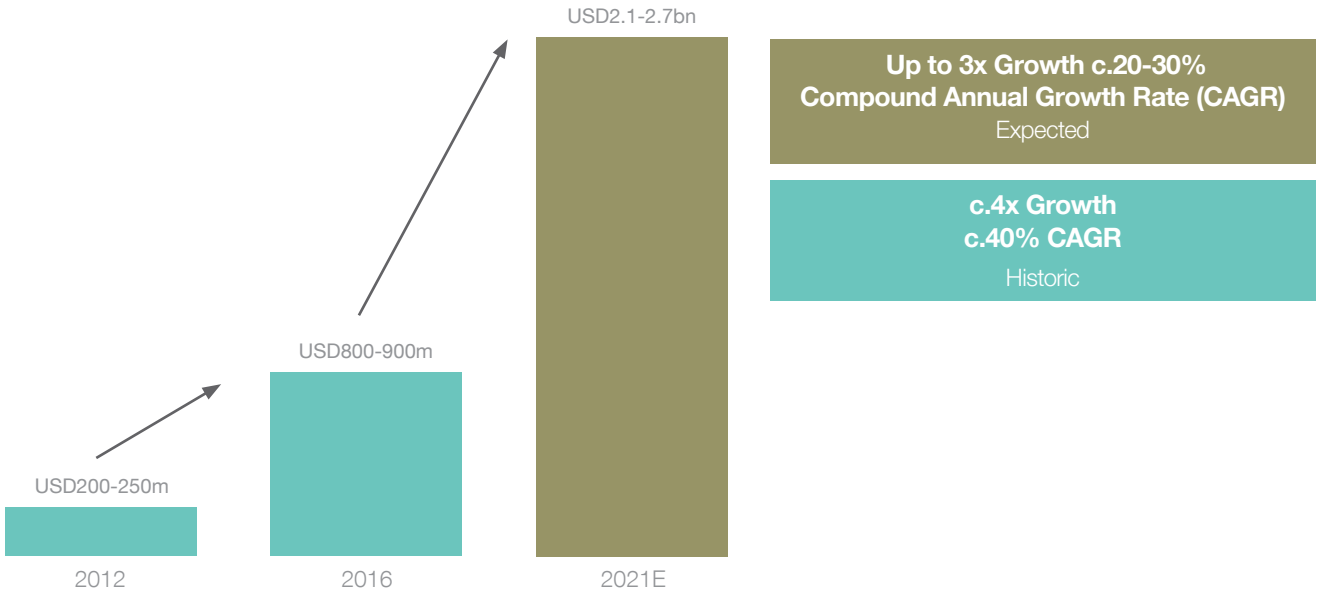
That case was followed in July 2018 by the Fortis settlement, which saw a Dutch court approve a USD1.5bn shareholder settlement with insurance company Aegis, the successor company of Fortis, over claims that Fortis over-invested in U.S. mortgage-backed securities before the financial crisis. The Fortis settlement is reportedly the biggest-ever for shareholders suing in Europe.

In Spain, investors raised claims against Bankia and its former directors for the provision of misleading information in the bank's IPO, driving growing concern in that market about directors' liabilities in relation to disclosure in capital markets transactions. Other shareholder actions that have taken off outside the U.S. include claims against Volkswagen, Petrobras and Toshiba.

Group claims, backed by third-party funders, are becoming a much more common feature of the European litigation landscape, particularly for cases involving environmental and human rights claims, antitrust, product liability and insolvency cases. The increased activity of claimant firms, along with the growth of litigation funders, makes this a burgeoning and potentially high-value new area of risk for corporates.

In October 2018, investment management firm Burford Capital published its annual Litigation Finance Survey, revealing a 237% increase in the use of litigation finance since its records began in 2012, and anticipating more growth on the horizon. Furthermore, based on publicly available information, global assets under management by 16 third-party litigation funders operating in the UK now stand at over GBP1.5bn. The actual figure is likely to be higher.

Annual dispute finance investment*



*Data has been provided by Vannin Capital

Increasing tax scrutiny

EU member states will need to apply five new legally-binding anti-tax avoidance measures as of 1 January 2019, following the adoption of the Anti Tax Avoidance Directive in late 2016. The new rules create a minimum level of protection against corporate tax avoidance throughout the EU, and come at a time of heightened tax scrutiny and a global clampdown on tax avoidance impacting both businesses and individuals.

In the UK, the Criminal Finances Act 2017 (the **Act**) represents the largest overhaul of the country's anti-money laundering and proceeds of crime regime in more than a decade and is the largest expansion of corporate criminal liability since the Bribery Act 2010. It imposes criminal liability on UK and non-UK businesses that fail to prevent the facilitation of UK or foreign tax evasion by an associated person. The new Act has extraterritorial effect, applying to any company that is incorporated under UK law, or has a permanent establishment in the UK, and will hold firms criminally liable if employees help others avoid foreign or UK tax.

Alongside the dangers of corporate tax evasion, and the new powers given to prosecutors under the Act, board members must also now deal with a growing threat associated with legal tax avoidance.

There is growing evidence that the threat by HMRC to apply diverted profits tax is causing companies to pay more tax than they are obliged to in order to avoid reputational harm.

Diverted profits tax is a relatively new tax introduced in the UK in 2015 to address public concerns about large companies booking profits in low-tax jurisdictions to avoid higher corporate tax rates in the UK. The rate is set at 25%, significantly higher than conventional corporate tax rate of 19%, and there is a requirement on companies to notify HMRC in the event that the arrangements they have in place could potentially fall under the legislation. Failure to notify can result in additional penalties. Notifications have risen steadily, from 48 in 2015/2016 to 220 in 2017/2018.

The challenge for directors comes in weighing up the competing responsibilities to pay all corporate taxes due, while not overpaying and failing to deliver returns to shareholders. Directors have a duty to promote the success of the company, and while legal tax avoidance may seem a legitimate means of increasing profits, they also have a duty under Section 172 to maintain a reputation for high standards of business conduct, which could be jeopardised by bad press related to tax avoidance.

Many other jurisdictions are similarly clamping down on tax avoidance, and the liabilities of directors for errors in tax returns continue to increase. Under Dutch law, for example, managing directors may be liable for specific taxes, social insurance contributions and contributions to mandatory pension schemes if the corporation has not correctly fulfilled its reporting obligation, with each managing director jointly and severally liable for the payment of the amounts due (unless the director can show that he/she is not to blame).

A facet of the globalisation of business is the growth of holding companies with a broad range of international interests and investments. Luxembourg is one of the principal centres for such companies in Europe:

Luxembourg holding companies and D&O

There are now many thousands of Luxembourg holding companies, with Sàrls being the most common form, that hold investments throughout Europe across different sectors. A particularly active sector in Luxembourg is the alternative investments market, with vehicles being established in Luxembourg to invest in private equity, real estate, hedge, infrastructure and credit funds. The Blackstone Group, one of the world's largest alternative asset managers, now has more than 1,000 Luxembourg holding companies, for example, and Oaktree Capital has more than 500.

The boards of Luxembourg holding companies can find themselves involved in contentious situations, when deals go wrong, or lenders seek to enforce and challenge distributions to sponsors. Most boards of Luxembourg holding companies in this sector comprise a combination of sponsor employees and independent Luxembourg-resident directors.

This raises several issues from a D&O coverage perspective, namely that:

(i) Board members (both sponsor employees and independents) often do not check, or are not allowed to check, whether they are covered by a suitable policy;

(ii) Insurance policies may not be drafted in a way that clearly covers the Luxembourg vehicles (as a result of the particular structures or types of vehicles used in Luxembourg, which can often be complex) and

(iii) People are not sufficiently clear on the limitations of insured risks under Luxembourg law (regulatory fines being excluded, for example).

Tackling cyber and data risk

On top of the growing burden of regulatory and enforcement risk, two other concerns continue to play heavily on the minds of directors and officers: those relating to cyber attack and data loss.

This year, for the first time, the risks associated with cyber attacks and data breaches top the list of risks that directors are most concerned about, overtaking regulatory and other investigations, which have been front of mind in every single one of our previous reports.

There are certainly signs that the risks of such incidents have increased, with **44% of our respondents this year saying that they have experienced either a significant cyber attack or a sizeable data loss in the past year. The comparable figure in last year's survey was just 24%, suggesting a doubling of occurrences**. Perhaps unsurprisingly, the perceived exposure is greater the larger the business: 47% of listed company respondents reported being impacted by a cyber event, and 48% of those working in large companies.

When asked to prioritise the risks facing their businesses, more than half of all those questioned (52%) described the risk of data loss, data breach or risks associated with the EU's new General Data Protection Regulation (GDPR) as very or extremely concerning. Exactly 50% ranked cyber attack as causing them the same level of anxiety. When combined – given that the two risks are so often inter-related – these two risks together become huge for business leaders.

This is no surprise given the fact that the GDPR came into effect on 25 May 2018, bringing with it onerous obligations, new penalties for breaches, and a raft of best-practice guidelines that few businesses were expected to be up to speed with immediately. Against such a backdrop, the frequent newspaper headlines reporting on cyber security breaches at major international corporations only serve to heighten the sense that attacks are always imminent, difficult to prevent, and potentially crippling.

Just a few of the most sophisticated cyber security incidents to have hit the headlines in the past 12 months include Russian hackers reportedly infiltrating and probing U.S. power companies; Iranian hackers attacking more than 300 universities around the world and stealing intellectual property worth USD3bn; and even Google being forced to close down its own social network Google+ after third-party app developers managed to access data from the friends of users.

In October 2018, the British Conservative Party saw its official conference app breached, revealing personal details of senior members of Parliament, while the month before, British Airways suffered a sophisticated data breach affecting 380,000 customers using its website and mobile app. And perhaps the most notorious incident of all was the revelation that millions of Facebook users had their personal information compromised by the election data company Cambridge Analytica, which apparently accessed Facebook profiles without the users' consent to target voters on behalf of both the Trump presidential campaign and for Leave EU.

Enforcement activity is clearly hotting up in the cyber arena as a result of public and political concern. In September, credit reference agency Equifax was fined GBP500,000 by the Information Commissioner's Office for failing to protect the personal information of up to 15 million UK citizens during a cyber attack in 2017. The fine was the maximum allowed under the Data Protection Act 1998, which was the law in force at the time that the cyber attack occurred. Meanwhile Mark Steward, Executive Director of Enforcement and Market Oversight at the FCA, said: "The FCA has no tolerance for banks that fail to protect customers from foreseeable risks.…Banks must ensure that their financial crime systems, and the individuals who design and operate them, work to substantially reduce the risk of such attacks occurring in the first place."

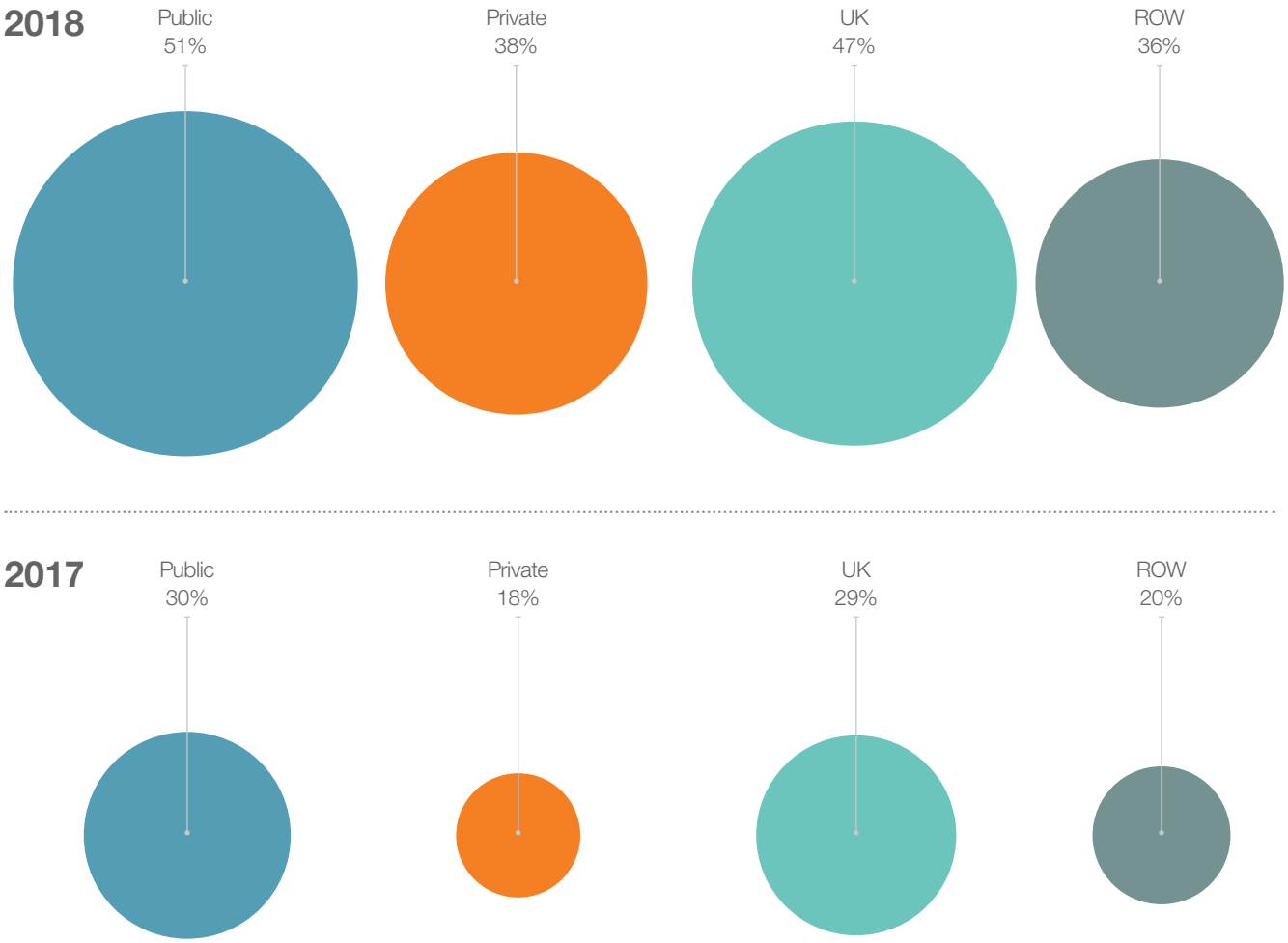
Philip Annett, Counsel at Allen & Overy LLP specialising in contentious regulatory matters, says the FCA is focused on risk management and the responses of senior managers in the context of cyber. He says: "We are seeing increasing scrutiny from the FCA on the robustness of firms' systems and controls to adequately respond to a cyber attack. In a lot of recent cases we have seen the existence of proper response plans, but those didn't work effectively when they were put to the test."

The GDPR now permits authorities to impose fines for some data infringements of up to 4% of annual worldwide turnover or EUR20m, and these increased fines are clearly capturing the attention of concerned executives.

"We are seeing increasing scrutiny from the FCA on the robustness of firms' systems and controls to adequately respond to a cyber attack. In a lot of recent cases we have seen the existence of proper response plans, but those didn't work effectively when they were put to the test."

Philip Annett, Counsel, Allen & Overy LLP

Experienced a cyber attack/loss of data



Some key things to keep in mind about the new GDPR requirements include:

– The GDPR has expanded territorial reach, and catches data controllers and processors outside the EU whose processing activities relate to offering goods or services to, or monitoring the behaviour of, European citizens.

– Data controllers and processors may need to designate Data Protection Officers as part of their accountability programme.

– The GDPR places onerous accountability obligations on data controllers to demonstrate compliance.

– Data processors now have direct obligations for the first time. They must, for example, maintain a written record of processing activities carried out on their behalf, designate a data protection officer where required, and notify the controller if they become aware of a personal data breach without undue delay.

– Consent must be freely given, specific, informed and unambiguous. Requests for consent should be separate from other terms and be in clear and plain language.

In its latest annual report, the UK Information Commissioner's Office highlighted the way in which data protection and privacy have moved up the agenda since 2017. The ICO issued the largest number and amount of civil monetary penalties ever in 2017/18, including 26 penalties totalling GBP3.3m for breaches of electronic marketing laws and 10 enforcement notices. In all, 11 fines totalling GBP1.3m were meted out for serious security failures under the Data Protection Act 1998, and there was a total of 19 criminal prosecutions, resulting in 18 convictions.

Who takes the lead?

One of the biggest challenges facing executives when it comes to cyber security is working out who takes the lead within the business, with many facing a 'specialist-generalist' dilemma: specialisation is necessary given the complexity of the issues, but everyone in the business needs to be up to speed on the critical nature of cyber resilience, and taking necessary steps.

In September, The Economic Intelligence Unit published the results of a global survey of over 450 companies around the world, sponsored by Willis Towers Watson, which found almost 40% of executives felt the board should oversee cyber, while 24% felt it should be the role of a specialist cyber committee.

The survey also found that communication across the leadership team on cybersecurity risks is often inconsistent, with only 8% of executives saying their Chief Information Security Officer (CISO), or equivalent, performs above average in communicating the financial, workforce, reputational or personal consequences of cyber threats.

Anthony Dagostino, global head of cyber risk with Willis Towers Watson, says: "Cyber resiliency starts with the board, because they understand risk and can help their organisations set the appropriate strategy to effectively mitigate that risk.

"While CISOs are security specialists, most of them still struggle with adequately translating security threats into operational and financial impact to their organisations – which is what boards want to understand. To close this communication gap, CISOs need tools that can help them quantify and translate the vulnerabilities uncovered from their cybersecurity maturity assessments," he says.

"Cyber resiliency starts with the board, because they understand risk and can help their organisations set the appropriate strategy to effectively mitigate that risk."

Anthony Dagostino, Global Head of Cyber Risk,
Willis Towers Watson

Addressing personal liability

The regulatory focus on individuals can now clearly be seen to be having a tangible effect on the way that companies conduct themselves. Most of our respondents say that the increasing spotlight on senior executives is changing their company's decision-making processes (60%), while half say that it is changing their company's appetite for risk. Here we see a divergence by company size – smaller companies are far more likely than larger firms to change their decision-making processes because of personal liabilities, but much less likely to adjust their risk appetite.

This year, as in previous years, the results of our survey are testament to the fact that claims and investigations against company directors are becoming more common, with 43% of respondents working in large businesses reporting experience of regulatory claims involving directors. While one in three of all those surveyed has experience of regulatory claims involving directors – a figure that is in line with last year's findings – we now see 38% of listed companies dealing with regulatory claims. Furthermore, 13% of our respondents have experience of criminal claims involving a director; a figure that rises to 14% for listed companies, and 18% among large employers.

While it remains a key principle of the English legal system that a company is a separate legal entity from its leaders, still there is a growing demand from politicians, shareholders, the media and the public for individuals to be seen to be punished when companies fail. The sight of company bosses in front of parliamentary committees answering for their actions has become much more common, and we have seen some business leaders standing criminal trial, or finding themselves on the receiving end of private prosecutions.

Since we began publishing this series, directors in the UK have seen their personal liabilities increase for offences relating to bribery, corruption and fraud; competition and antitrust matters; environmental law; data protection; health and safety; tax; sanctions; money laundering; financial reporting requirements and modern slavery. They are also increasingly subject to the extraterritorial reach of U.S. regulators, including via the massive consumer protection legislation contained in the Dodd-Frank Act.

Given the focus on corporate head office location, not least in the context of Brexit and passporting under European Union rules, there may be opportunities for jurisdictions to make themselves more attractive locations to domicile by reducing the scope of personal liability. A radical proposal in the draft Belgian Companies Code, for example, suggested a cap on director liabilities (see boxout).

Operational risks also feature highly among directors' greatest concerns, with health and safety legislation and its impact on company business now a top-five worry. Class action lawsuits against the company and its directors are also seen as a significant risk, as are employment practice claims around equal pay, discrimination and similar issues.

Belgium proposes cap on directors' liabilities

A radical proposal in the new draft of the Belgian Companies Code has attracted attention internationally, with plans to introduce a cap on the director liabilities of Belgian companies of up to EUR12m, depending on company size. This proposal, driven by an effort to make Belgium a more competitive and attractive place for the establishment of businesses, could be a sign of things to come, as jurisdictions work to differentiate themselves and attract corporate HQs.

The Belgian government hopes parliament will adopt the proposal before the end of 2018, further justifying the cap as a way to ensure Belgium does not miss out on talented directors in the international war for talent, and as a means of ensuring directors' liability risks can continue to be insured at acceptable terms and conditions.

Serious Fraud Office activity

As the pressure grows on UK law enforcement agencies to crack down on corporate offenders, it has become increasingly likely that companies will find themselves on the receiving end of interest from the Serious Fraud Office. According to a Freedom of Information request, the number of Section 2 notices issued by the SFO has more than doubled in the last five years, and for 2017/18 stood at 1,032. Section 2 notices are used to compel witnesses or suspects to provide documents or information to the SFO, and there were 463 issued in the year 2013/14. The number jumped by 41% last year alone, from 730 cases in 2016/2017.

Section 2 notices have become increasingly powerful weapons, with the concept of 'documents' interpreted broadly to apply to computer records. Moreover, the UK courts have recently confirmed that section 2 notices have extraterritorial effect and can be applied, in appropriate cases, both to companies and/or documents outside the UK.

The new SFO Director Lisa Osofsky, who began her five-year term at the end of August 2018, previously worked with compliance firm Exiger after a career as a U.S. federal prosecutor pursuing white collar crime cases. She is now expected to focus her attentions (among other things) on money laundering investigations, where the SFO received 112 reports in 2018, up from 19 in 2017 and the highest figure over the last five years.

According to a Freedom of Information request, the number of Section 2 notices issued by the SFO has more than doubled in the last five years, and for 2017/18 stood at 1,032. Section 2 notices are used to compel witnesses or suspects to provide documents or information to the SFO, and there were 463 issued in the year 2013/14.

Criminal cartel enforcement

Cartel enforcement actions around the world continue to grab headlines, with the European Commission last year breaking the USD2bn barrier thanks in large part to the fine imposed on Scania in the trucks investigation (EUR880m). Since April 2014, the law in the UK has changed to remove the dishonesty requirement in prosecuting criminal cartel offences, but there have yet to be any prosecutions despite this lower burden of proof. An increase in budget may help the Competition and Markets Authority (CMA) pursue more cases, though there remains a resourcing question around Brexit.

Eve Giles, a partner at Allen & Overy LLP with over 20 years' experience advising on high-profile criminal investigations, says she expects more criminal cartel cases moving forward. "I anticipate more criminal cartel activity. In the wake of Brexit, I think the CMA will be looking to assert itself. Some commentators suggest that there might be fewer investigations as a result of Brexit, but my view is that we will see more activity on the criminal side from all the UK regulators."

"I anticipate more criminal cartel activity. In the wake of Brexit, I think the CMA will be looking to assert itself. Some commentators suggest that there might be fewer investigations as a result of Brexit, but my view is that we will see more activity on the criminal side from all the UK regulators."

Eve Giles, Partner, Allen & Overy LLP

Employment claims

Employment claims have been in the spotlight following the global #metoo movement sparked by concerns around harassment or sexual discrimination in the workplace. In all, 30% of respondents to our survey regarded employment practice claims as an extremely important or very important concern, compared with 22% of respondents who felt the same last year.

In the UK, there has been an increase in employment tribunal cases in the past year, since fees were scrapped in July 2017. Figures released by the Ministry of Justice showed a 118% increase in claims in the period January to March 2018 when compared to the same period in 2017, with that increase up from a 90% increase the previous quarter, suggesting the pace of the uptick in claims is accelerating.

There are also signs that the already broad remit of financial services regulators in the UK will be extended to cover a much wider group of concerns than merely financial crime and misconduct, including the use of regulatory powers to tackle sexual harassment and other employment practice issues. Speaking to the Women and Equalities Committee in Parliament in 2018, the FCA's Director of Supervision – Investment, Wholesale and Specialists, Megan Butler, said: "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, an environment where the best business decisions get taken, the best risk decisions get taken." She added: "We do not compartmentalise that away from a consideration of what makes an individual fit and proper and we expect firms to take all those aspects into account when they look at whether their key individuals are fit and proper to do their roles."

The FCA's Director of Supervision – Investment, Wholesale and Specialists, Megan Butler, said: "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, an environment where the best business decisions get taken, the best risk decisions get taken."

Senior Managers and Certification Regime

The UK's Senior Managers and Certification Regime (SM&CR) forms a key tenet of the FCA's drive to improve culture, governance and accountability in financial services firms. First introduced in March 2016, it is one of the key pieces of legislation that works to deter misconduct in the financial services industry by improving personal accountability, and it will be extended to cover all insurance and reinsurance firms regulated by the FCA and the Prudential Regulation Authority (PRA) from 10 December 2018, and will further apply to all firms authorised by the Financial Services and Markets Authority as of 9 December 2019.

The SM&CR is focused 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 latest extension of the regime marks a significant expansion of the focus on senior individuals through the imposition of personal liabilities. The FCA's intentions are clear, with it currently opening more cases than ever before, particularly focused on financial crime.

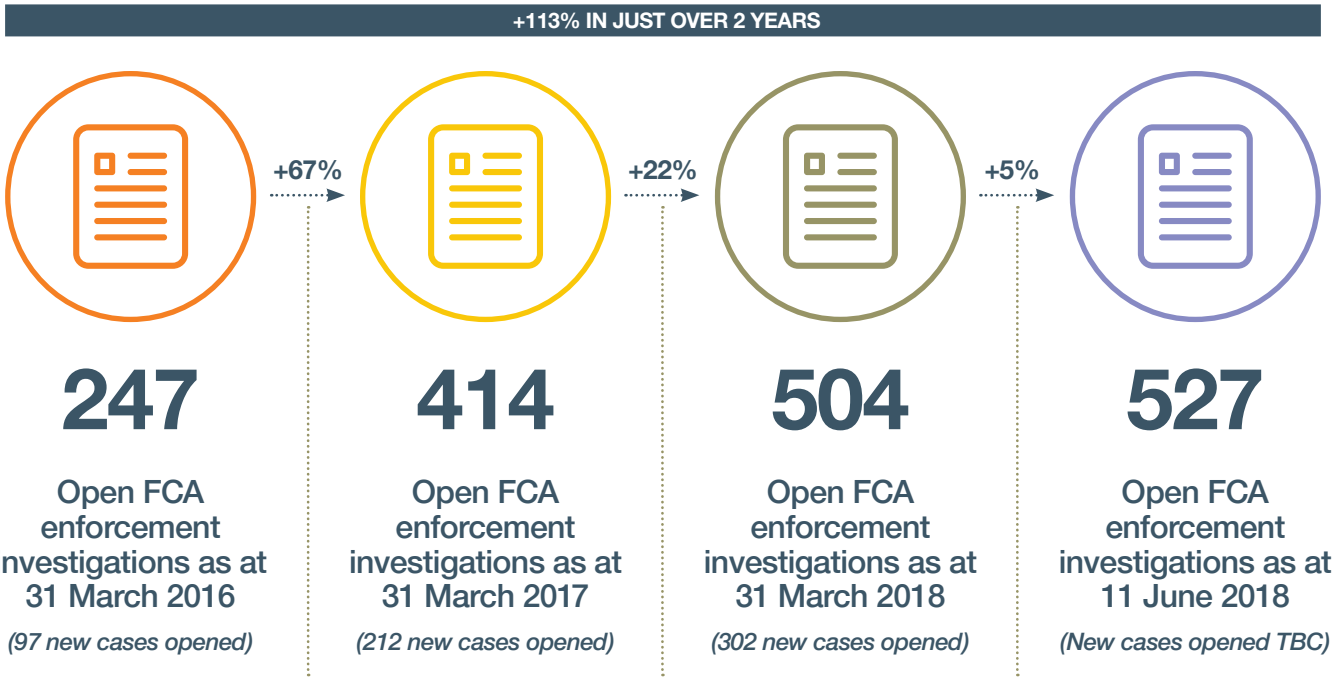
As of 31 March 2018, according to its annual enforcement report, the regulator was dealing with 504 investigations into both individuals and firms, compared with 414 a year previously and 247 at the same point in 2016.

The expanded caseload included 86 investigations looking into suspected financial crime and another 75 on insider dealing, where the FCA has the power to criminally prosecute. A further 61 cases were linked to culture and governance, where the FCA has been focusing its efforts and where there was a fourfold increase from 15 cases the year before.

There is also evidence of an enhanced focus on individuals. According to a Freedom of Information request submitted by Allen & Overy LLP in June 2018, of 527 active cases open at that point, 306 related to individuals, or 58%. At that time the FCA had five senior managers under investigation and 10 certified persons. At the same point, the PRA had 22 active cases, of which 14 were enforcement investigations into individuals.

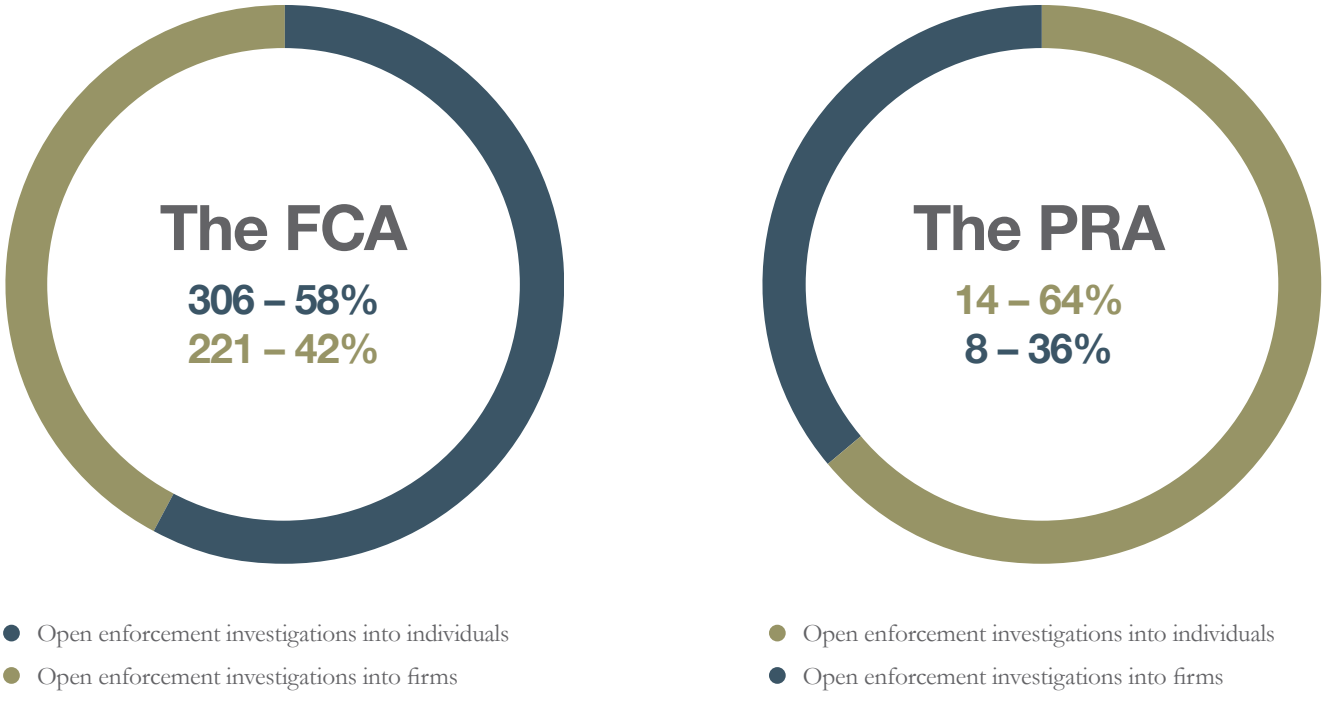
As of 31 March 2018, according to its annual enforcement report, the regulator was dealing with 504 investigations into both individuals and firms, compared with 414 a year previously and 247 at the same point in 2016.

The number of open FCA investigations continues to increase



Source: FCA Annual Reports and Freedom of Information Act request submitted to the FCA by Allen & Overy

Investigations into individuals represent a significant proportion of both regulators' current* investigations



Source: Information obtained via Freedom of Information Act requests submitted by Allen & Overy | As at June 2018

The UK Corporate Governance Code

In July 2018, the UK's Financial Reporting Council (FRC) published the 2018 UK Corporate Governance Code, setting out the relationship between companies, shareholders and stakeholders in a shorter and more concise version. The Code was first introduced in 1992 and has been updated many times since, but the latest changes are the most extensive ever made.

The Code places a lot of emphasis on companies establishing a corporate culture that is aligned with the company purpose and strategy, and that promotes integrity and values diversity. There is a new provision to drive greater board engagement with the workforce to understand their views – the Code asks boards to describe how they have considered the interests of stakeholders when performing their duties under Section 172 of the 2006 Companies Act.

This section of the Companies Act imposes a duty on directors to promote the success of the company, while considering:

- The likely consequences of any decision in the long term
- The interests of the company's employees
- The need to foster the company's business relationships with suppliers, customers and others
- The impact of the company's operations on the community and the environment
- The desirability of the company maintaining a reputation for high standards of business conduct
- The need to act fairly as between members of the company

Last year, the House of Commons' Business, Energy and Industrial Strategy Committee considered strategies to reinforce Section 172 duties, as the section has been seen as a toothless tiger, with no successful proceedings having so far been brought against directors for failure to comply with its principles. The new code now states that corporate governance reporting should include providing information that 'enables shareholders to assess how the directors have performed their duty under section 172.'

This will be backed up by new secondary legislation (the Companies (Miscellaneous Reporting) Regulations 2018) which will require large companies to report on how the directors have had regard to the company's key stakeholders when performing their duty to promote the success of the company. Both the Regulations and the new Code will apply to accounting periods beginning on or after 1 January 2019.

Companies should therefore be prepared to articulate the ways in which they have considered things like the interests of employees and the impact of their operations on the community and environment. In October 2018, the GC100, which represents general counsel and company secretaries working in the FTSE100, published the first guidance for company directors on the practical interpretation of section 172, aimed at supporting directors in discharging their legal duties beyond their commitment to shareholders' interests.

Insolvency risk

Against a challenging economic backdrop, more than a quarter of those that completed our survey considered the risk of insolvency or corporate collapse to be very or extremely important in their business. Here, again, we see a spotlight being shone on directors and officers, who have been criticised in a number of recent high-profile corporate collapses, most notably for failings in the management of pension scheme liabilities.

In a similar vein, the UK government has now put forward proposals to extend the responsibilities of directors of parent companies to consider the future viability of subsidiaries after sale.

The government's proposal says that: "Holding company directors should be held to account if they conduct a sale which harms the interests of the subsidiary's stakeholders, such as its employees or creditors, where that harm could have been reasonably foreseen at the time of the sale."

The sanctions proposed for breach of the new law include a power granted to liquidators and administrators to order that a director contribute a sum that the court thinks fit towards the subsidiary's creditors, and that the director should also be liable to be disqualified if appropriate.

Protecting directors and officers

Insurance market trends

Given the ever-expanding slate of personal liabilities to which senior executives are now exposed, both regulatory and otherwise, the attention being paid to D&O policy coverage and related indemnities grows year-by-year. Senior managers are well advised to deal with the new regulatory focus on their personal behaviours by taking individual responsibility for understanding the best personal liability protection available to them through insurance and their employer's indemnity.

Several London marketplace realities are impacting the D&O market and should be borne in mind in this context. For a start, 2017 has been the worst year for U.S. securities class action filings since the dotcom bubble in 2001 and has led many insurers to review capacity and rating for U.S.-exposed clients.

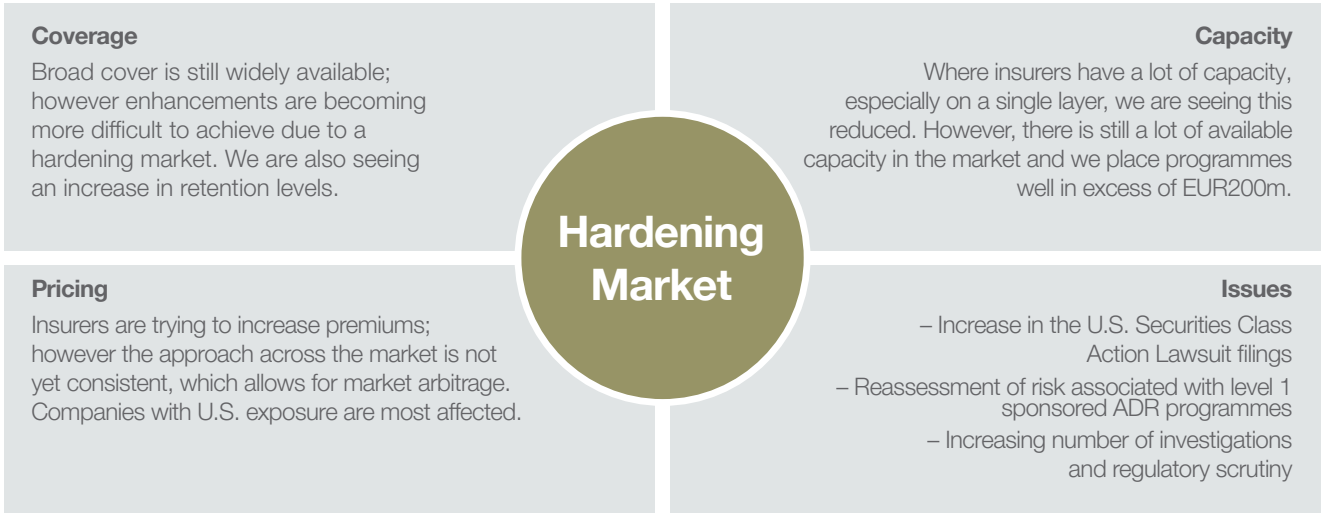
Significant claims activity has also occurred in other parts of the world, most notably Australia, where claims significantly exceeded premium levels. Meanwhile, the continuing trend of regulatory enforcement is placing pressure on primary and low excess layers, and most major primary insurers in the London market are now close to or above 100% combined ratio in commercial D&O.

Insurers have also experienced significant losses across other lines of business, including losses attributable to a particularly severe hurricane season. This has increased total combined ratios across all global lines above 100% for many and negatively impacted profitability for most carriers.

When it comes to the London D&O insurance market, there are clear signs of hardening thanks to increased claims activity involving company directors. Whether or not directors are ultimately held liable, the associated defence costs can be extremely expensive, and the litigation or regulatory process can take months or even years to be resolved. This has an impact on the insurance market in terms of the available capacity, cover and pricing. Consequently, insurers have been increasing premium rates and retention levels as well as re-evaluating their portfolios and reducing capacity. That is especially so for listed companies and for those with significant U.S. exposure.

Significant claims activity has also occurred in other parts of the world, most notably Australia, where claims significantly exceeded premium levels.

Insurance market trends



Policy priorities

Every year, as part of this survey, we ask our respondents about their priorities when it comes to securing D&O cover. The rising threat of international exposure is clearly evident here, with the ability of a D&O policy or company indemnification to respond to claims in ALL jurisdictions being the chief concern for respondents for the first time.

Also rising up the agenda is a broad definition of who is insured, which has not previously featured in the top five worries for those completing our survey. Clear and easy to follow policy terms, which have been the first priority for respondents every year since 2013, dropped to fourth in the list this year. It would be nice to think that this fall is attributable to an improvement in the clarity of D&O policy terms, but it is instead more probably attributable to an increase in concerns felt in other areas.

One sometimes uncomfortable truth about D&O insurance is that it is trying to cater to more than one set of interests. On the one hand, it offers balance sheet protection to the company itself in the form of reimbursement in respect of indemnities paid to its employees. On the other, it is expected to operate as the failsafe mechanism for the directors and employees themselves in the event that the company does not pay. The findings of our survey shed some interesting light on this dichotomy.

If you break down by job description the answers to the questions asking respondents to identify key priorities with respect to D&O insurance, you see senior executives, directors and NEDs much more interested in how claims against D&O policies will be controlled and settled. On the key threshold issues, there is a clear difference between the individuals who enjoy the benefit of the cover and those generally responsible for its administration, such as risk and compliance managers.

For principals and directors, key priorities include clear and easy to follow terms (61/63%) and other issues 'at the sharp end', such as control and access to the policy for directors (61% for directors) and the ability of insurers to avoid the policy for non-disclosure (61% for directors). For the rest, issues such as whether there is cover for fines and penalties (62%) and understanding how disputes with insurers will be dealt with (59%) are of greater concern.

Unsurprisingly, for this group, the implications of company insolvency, the depletion of insurance limits and what happens when they retire are all less of a concern.

More difficult to explain at first glance is the finding that directors and principals are more concerned about competitive pricing than the other respondents. After all, it is usually the company that pays the premium. Perhaps directors and principals who are less likely to be aware of prevailing market conditions are simply expressing a general value for money concern.

Other findings are also a little surprising. For example, only 52% of directors are concerned about how the policy reacts in the event of a conflict of interest (and the number is even smaller among other respondents), yet this issue unless addressed has the potential to create a gap in cover in which neither the company nor the insurers pay for defence costs. Similarly, less than 50% of directors and principals are worried about rapid depletion of limits even though the limits are usually shared with the company and other employees.

All of this perhaps suggests that more work needs to be done by the insurance industry to explain some of the issues to the various stakeholders that comprise the buyers of D&O insurance, such as how insurers rate risk; how the D&O policy operates in a claims context; and the practical and legal challenges that large claims can give rise to.

A guide: practical tips on D&O and indemnities

Indemnification and insurance products: mind the gap

The two key protections 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 from company to company.

With more than one way of getting protection, this year, nearly half of our respondents expressed a concern about the coordination of their D&O policy with their company's indemnification obligations. Last year, we found that a quarter of respondents were concerned about this issue, and so the challenge is clearly front of mind.

There are important lessons to draw from the gaps that exist between these protection products, as the table below shows

Gaps in a D&O insurance policy	Gaps in an indemnity contract with the company
D&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 if, the company is also included in the claim, confusion can arise (as the company may have narrower coverage than the individuals, or no coverage at all). Cover is often complex and comes with built in restrictions and exclusions.	An individual has no automatic right to an indemnity. Rights to an indemnity may be further limited by: (a) statutory restrictions (eg companies cannot indemnify for any penalties that the director incurs under criminal or regulatory proceedings); (b) the terms of any relevant employment contract (or the indemnity itself); (c) the company's willingness and appetite to indemnify based on: (i) its perception of the facts in each case; and (ii) whether the senior manager is still 'in post' when the indemnity is called upon.
The insurance limits are usually shared between a large group of individuals (which is not restricted to senior executives, and often includes the company itself). The limits are therefore prone to rapid depletion and even exhaustion.	The company indemnity will be worthless in the event of company insolvency (D&O can cover in this case). The indemnity may not continue after the individual has ceased to be employed. Even if it does, the terms may not be as generous.

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 ten-point checklist that covers the most important questions that senior individuals may wish to consider with their employees.

A ten point checklist: some important questions that senior individuals may wish to consider with their employees

1. With which categories of employee, and 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. 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?
7. 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?
8. 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?
9. 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?
10. 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;

– 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).

However, a D&O insurance policy will be subject to policy exclusions and an aggregate policy limit that does not appear in typical indemnity arrangements. Further, 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 (although 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.

However, 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 a D&O insurance policy nor an indemnity contract with the company can do for you

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

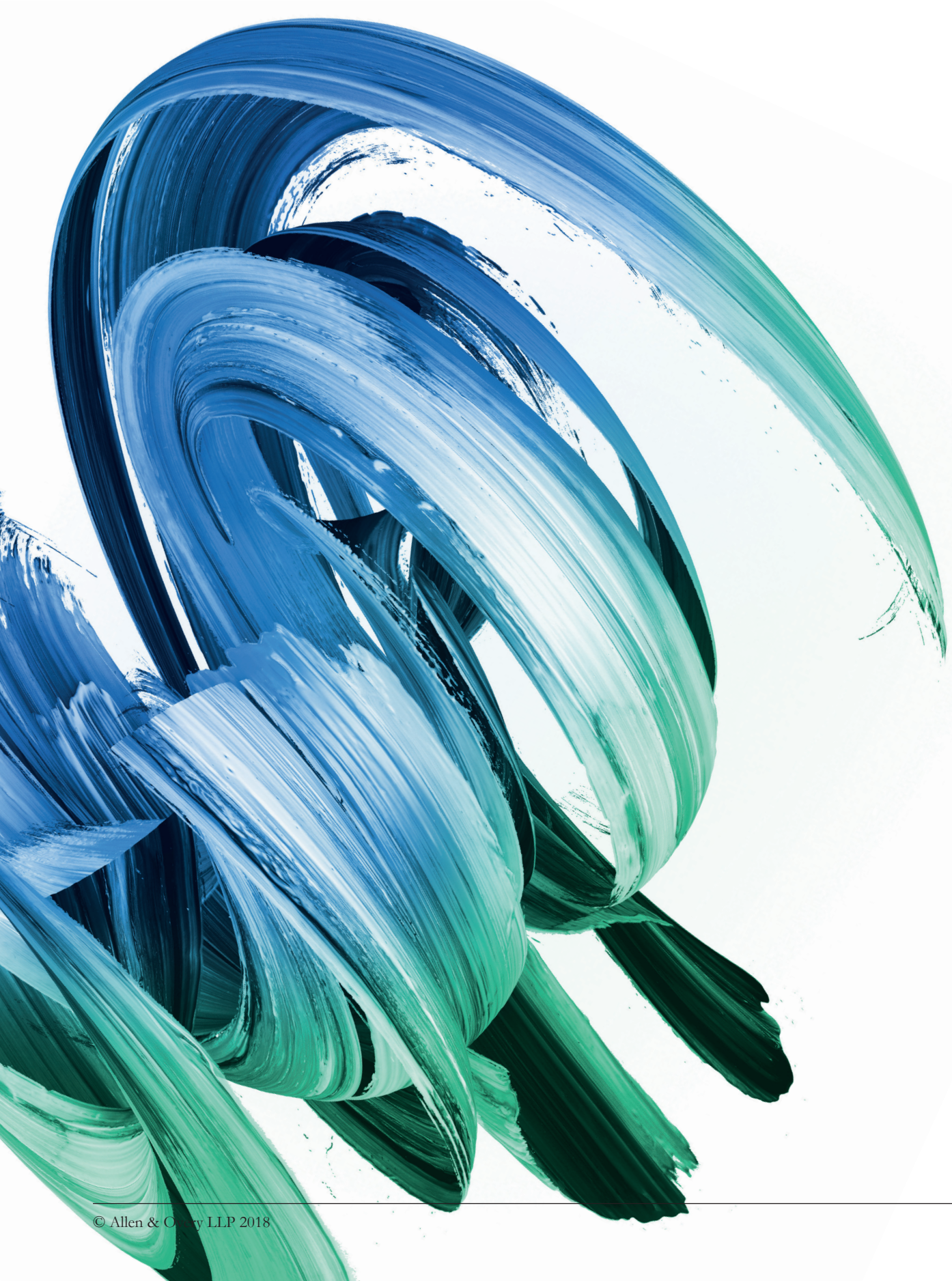
– liability arising by reason of the director's dishonest, fraudulent or criminal conduct; or

– criminal fines or regulatory penalties.

Allocation clauses

While most purchasers of D&O policies typically believe a policy should pay all costs reasonably related to the insured person, in fact, that is not always the case. An allocation clause will typically state that when an underlying claim includes both covered and uncovered matters, or both covered and uncovered parties, then the insurer and the policyholder will do their best to agree on an allocation between loss that is covered, and loss that is not. In the absence of an agreement, an allocation clause will normally set out that the issue will be resolved by arbitration.

This raises the question of what principles apply in determining how much of the mixed costs are covered in any given case, which can be a major issue for large regulatory investigations where directors and senior executives are represented by the same lawyers as those representing the company. This can sometimes be addressed by contractually pre-agreeing the proportions, but there may be premium considerations involved in going down that route. Executives would be well advised to be aware of this issue at the outset.



GLOBAL PRESENCE

Allen & Overy is an international legal practice with approximately 5,500 people, including some 550 partners, working in 44 offices worldwide. Allen & Overy LLP or an affiliated undertaking has an office in each of:

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

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. The term **partner** is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings.

allenovery.com