ALLEN & OVERY

Directors' liability

D&O: Entering uncharted territory

A survey conducted by Allen & Overy
and Willis Towers Watson | September 2017

Willis Towers Watson

Contents

Introduction

Welcome to this the fifth edition in our series of surveys on directors' liabilities, brought to you by the international law firm Allen & Overy LLP and the global advisory broking and solutions company Willis Towers Watson.

We began this exercise back in 2011 when – fresh from the throes of the global financial crisis – directors and high-ranking executives in public and privately-held corporations were feeling particularly exposed to liability and subject to an unprecedented degree of scrutiny. That said, the incidence of actual criminal, civil or even regulatory proceedings against individuals was still vanishingly small. To plug that perceived accountability gap the last six years have seen a steady increase in laws and regulations aimed at senior executives.

Over the following pages, we have revisited several of the themes that have consistently presented themselves in previous years, as well as highlighting several new developments that add to the breadth of concerns keeping directors and officers awake at night. We have looked not only at the risks and exposures facing business leaders, but also how well they feel their insurers are responding. In all, we surveyed 127 directors, non-executive directors, in-house lawyers, risk officers and compliance professionals, working in companies operating all over the world. We thank them all for taking the time to complete our survey and allowing us to create this market snapshot.

As we publish our fifth instalment of this research, and draw on six years' worth of data, we can identify some themes and trends emerging around the subject of boardroom sentiment. We continue to see regulators driving further and further forward with an agenda of personal accountability. The number of respondents to our survey that have experienced a claim or investigation involving a director of their company continues to grow, reaching over one in three this year, as against one in five as recently as 2014.

What does make it on to the agenda of directors and officers this year for the first time is the uncertainty surrounding macro-economic events: 38% of our respondents identified concerns in a post-Brexit landscape among the risks of greatest significance to their business, and 59% told us the current geo-political uncertainties create a significant additional risk to their businesses. This is why we have called this year's report *Entering Uncharted Territory*.

There are other new risks on the horizon for executives from a regulatory standpoint too, and in this year's survey we once again drew our respondents' attention to several new pieces of proposed and actual legislation that serve to expand the risk of personal liability. For example the Financial Reporting Council's proposals to extend its sanction regime to all directors of UK listed companies, the General Data Protection Regulation, and the individual personal liability that board members can incur for incorrect tax returns in some jurisdictions, such as Italy, Germany and Greece.

When it comes to D&O protection, our respondents continue to tell us that they want policy terms that are clear and easy to follow, and this year many are also focused on restricting insurers' ability to refuse a claim based on non-disclosure. Many worry about how claims against directors and officers will be controlled and settled, about whether their D&O policy and company indemnification will be able to respond to claims in all jurisdictions, and about the coordination of the D&O policy with a company's indemnification obligations. Given the rising levels of personal liability, it is little surprise to see these issues on the agenda of directors and officers around the world.

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 us and with your usual contact at either Allen & Overy LLP or Willis Towers Watson.

Both Joanna and Francis would like to extend particular thanks to Madison Kaur, Emma Waters and Patrick Mayock from Allen & Overy LLP in connection with the analysis of data and writing of this report and Elliott Harvey and Bonita Johnson from Willis Towers Watson with their assistance on the survey.

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

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

Executive summary

Our key findings

When conducting the research for this year's survey, we interviewed 127 individuals, comprising directors, non-executive directors, in-house lawyers, risk officers and compliance professionals.

Our respondents were split roughly equally between public and private companies and were spread across a wide variety of industries. In all, 37% were based in companies that conduct the majority of their business in the UK, while 33% described their businesses as global, 21% operated across EMEA, 6% in the U.S. and 5% in Asia Pacific.

A number of key themes emerge from the statistics and analysis contained in the following pages:

Over a third of respondents to our survey (33%) have **experience of a claim or investigation** involving a director of their company, up from 27% a year ago

Nearly one in four (24%) has experience of a **cyber attack or loss of data** significant enough to have been brought to the attention of the board in the last 12 months

Only 43% are aware of the Financial Conduct Authority's proposals **to extend the Senior Managers Regime** to all directors of FCA regulated UK companies

Nearly a quarter (24%) are not aware of the implications of the **General Data Protection Regulation** for their business

Some 78% of those who responded are not aware of the **individual personal liability** that board members can incur for **incorrect tax returns** in some jurisdictions, such as Italy, Germany and Greece

When it comes to D&O policy coverage, directors are most concerned that their policies have **clear and easy-to-follow policy terms**; that they **restrict insurers' ability to refuse a claim based on non-disclosure**; and as to how claims against directors and officers will be **controlled and settled**

Top five risks to directors, year-on-year

Top five policy coverage issues, year-on-year

Addressing personal accountability

In each of our last four reports analysing the state of directors' liabilities in the UK and abroad, we have considered in some depth the way in which regulators and policymakers around the world have focused their attentions on directors and officers in their efforts to improve corporate behaviours. Driven by public and shareholder pressure in the wake of the financial crisis, enforcement agencies have prioritised individual responsibility in the face of corporate wrongdoing, and have repeatedly promised to come down harder on offenders.

Over the last decade we have witnessed a proliferation of new regulations affecting directors and officers. Today this trend shows no signs of abating. Since we began publishing this series, directors in the UK have become personally liable for new offences that include bribery, corruption and fraud; competition and antitrust matters; environmental law; health and safety; sanctions; money laundering; financial reporting requirements; and Dodd-Frank and other extra-territorial U.S. legislation. There are more new corporate offences to come such as under the Criminal Finances Act, as to which, see below.

While the principle that a company is a separate legal entity from its leaders remains a key tenet of the English legal system, directors and officers are the subject of ever-expanding personal liabilities. There have been 19 charges* for corporate manslaughter since the Corporate Manslaughter and Corporate Homicide Act 2007, of which several included individual prosecutions for gross negligence manslaughter although all of these so far involve only small companies. We may see more high profile cases following the Grenfell Tower disaster. The sight of corporate leaders responding in person to challenging questioning in parliamentary inquiries into the behaviour of their business or industries is no longer unusual.

What's more, the growth of third-party litigation funding on the UK legal scene over recent years has made it easier for litigation against directors to get off the ground. The perceived success of a group of RBS shareholders in securing settlements in relation to claims against the bank and its bosses over a GBP12bn cash call in 2008, claims which were backed by third-party funding, may encourage more claims against business leaders.

This year, as in every previous edition of this report, our respondents tell us that the greatest risk they face remains the threat of regulatory and other investigations and inquiries – today 82% of those questioned consider such a risk to be significant for their business and its directors, up from 71% a year ago. And this fear is increasingly borne out in practice: this year we see a fairly significant increase in the number of respondents saying that they have had experience of a claim or investigation involving a director of their company.

Today, over one in three directors and officers has had such an experience; up from one in four a year ago, and one in five in our 2014 report. This figure rises to 39% for public companies compared to 28% in private companies, and 36% for UK companies as against 31% for companies that are global or conduct most of their business outside the UK.

When we compare these results against the data in our 2016 survey, the results are remarkable. The number of private companies experiencing a claim or investigation involving a director of their company has risen from 10% in 2016 to 28% in 2017. Similarly, while only 21% of UK companies had experience of a claim or investigation in 2016, that figure is now 36% indicating that personal liability for directors is of particular focus in the UK.

"The sight of corporate leaders responding in person to challenging questioning in parliamentary inquiries into the behaviour of their business or industries is no longer unusual."

*This is based on a Freedom of Information request and the figure is correct as of 18 February 2016

Have you had experience of a claim or investigation involving a director of your company?

Some risks have however dropped down the corporate agenda despite remaining very real: not one of our respondents named extradition as being of significance to its business and its directors, even though several years ago that was a much bigger worry (and reflected in our data, when in 2013 and 2014, 19% of respondents named extradition as being of significance). That response was at a time Ian Norris, the former chief executive of FTSE 250 engineering company Morgan Crucible, was extradited to the U.S. and sentenced to 18 months in jail for conspiring to obstruct a price-fixing investigation. Extradition risk has not gone away, even if it has moved out of the headlines and has therefore perhaps dropped off business leaders' bandwidths for the time being.

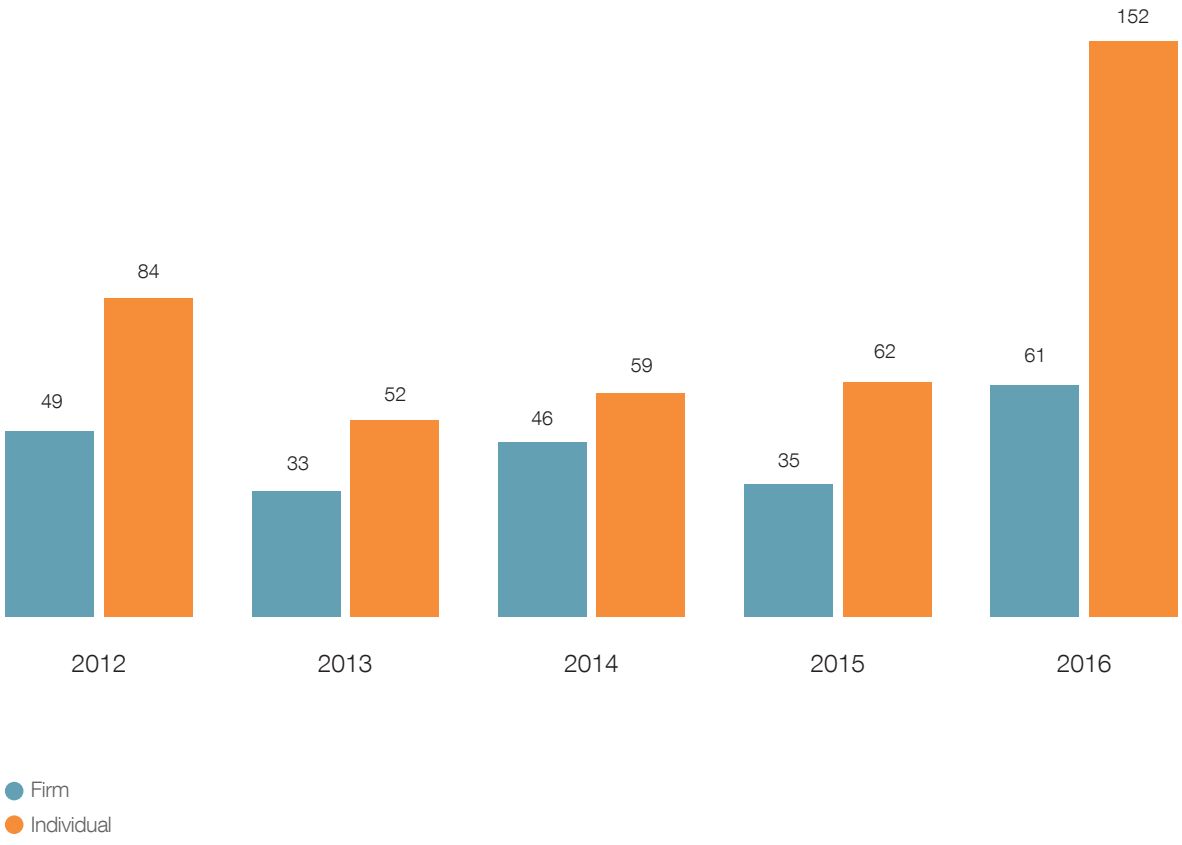
Likewise, the multiplicity of sanctions regimes no longer features among the risks that executives consider to be most pressing for their businesses, with only 23% naming them (compared with over 40% in our 2014 survey). This is perhaps surprising when the sanctions risk remains as complex as ever and the danger of draconian penalties has not receded.

Finally, while only 15% of our respondents consider environmental claims to be of any real concern, natural catastrophes have consistently ranked among the top five global business risks, and many argue it is only a matter of time before we see litigation against directors for failure to recognise, disclose or take steps in relation to a foreseeable climate-related risk.

Despite this already highly-fuelled backdrop of personal liabilities, lawmakers show no signs of slowing a drive towards holding directors and officers to account. Here we examine some of the newer risks moving up the corporate agenda, and note, with little surprise, the extent to which business leaders are increasingly struggling to keep abreast of their ever-expanding exposures.

Investigations against individuals by The Financial Conduct Authority per year

The Financial Conduct Authority's (FCA) own statistics, bear out our respondents' experience. The FCA's data shows a significant increase in the number of investigations opened against individuals whereas those against firms have remained largely static. This reflects what the FCA has recently described as its 'evolving approach' to investigations.




N
NE
E
S
SW
W
NW

The Senior Managers and Certification Regime

The UK's Senior Managers and Certification Regime (SM&CR) came into force in March 2016 as part of a shift in focus by the FCA towards individual accountability as a means to foster good governance and conduct culture in the financial services industry. The SM&CR has resulted in significant changes to the way in which individuals working in firms are regulated.

Currently applicable to UK banks, building societies, credit unions, Prudential Regulatory Authority (PRA) investment firms and branches of foreign banks operating in the UK, it will apply to all other FSMA-authorised firms – including insurers (who currently apply a revised version of the FCA's Approved Persons Regime and the PRA's Senior Insurance Managers Regime), investment firms, asset managers, insurance and mortgage brokers and consumer credit firms – can expect that the new regime will apply to them from some point in 2018. On 26 July 2017, the FCA published their consultation paper on extending the SM&CR (with a separate consultation paper for insurers) and are seeking responses by 3 November 2017.

While individuals who fall under the senior managers regime will continue to be pre-approved by regulators, firms are required, amongst other things, to ensure that they have procedures in place to assess the fitness and propriety of senior managers before applying for approval, and at least annually afterwards. Similar procedures must also be put in place for individuals who could pose a risk of significant harm to firms or their customers (eg staff who give investment advice) under the certification regime. In addition, in March this year new conduct rules were extended to apply to all staff (other than those in ancillary roles) and new regulatory reference rules came into force. As a result, firms have significantly increased responsibilities in relation to individuals who fall within the SM&CR regime. At the same time, a much wider group of individuals are now exposed to the risk of potential FCA or PRA enforcement action.

It will be particularly interesting to see how the extension of the SM&CR will affect the number of investigations that the FCA opens. As of the end of February 2017, the FCA disclosed (by way of a freedom of information request) that they had opened investigations into two individuals who are Senior Managers, and eleven investigations into former Approved Persons who are now likely to have transitioned into the Certification Regime.

As of the end of February 2017, the FCA disclosed (by way of a freedom of information request) that they had opened investigations into two individuals who are Senior Managers, and eleven investigations into former Approved Persons who are now likely to have transitioned into the Certification Regime.

Financial Reporting Council plans

Following on from the FCA's approach, what appears to have passed under the radar of many of our respondents is the Financial Reporting Council (FRC)'s proposals to extend its sanctions regime to all directors of UK listed companies who preside over serious accounting irregularities – something of which only 43% of our respondents were aware. These proposals were contained in the FRC's response to the Department for Business, Energy and Industrial Strategy's Corporate Governance Reform Green Paper, which set out Prime Minister Theresa May's agenda for more accountability on boards.

The FRC has yet to flex its muscles in terms of being an active enforcer of good corporate behaviour, but in its response it proposes wide-ranging powers be given to it for oversight of all directors. It is proposing the ability to sanction all listed company directors, not only those that are professional accountants, auditors or actuaries, where it already has disciplinary powers.

The House of Commons' Business, Energy and Industrial Strategy Committee has since published its recommendations on corporate governance arising out of responses to its Green Paper and notes that Section 172 of the Companies Act 2006 – the duty to promote the success of the company – has been in force for almost ten years, and yet during that time there have been no reported cases of shareholders bringing claims under that section. It goes on to recommend that the Government brings forward legislation to give the FRC the additional powers it needs to engage and hold to account company directors in respect of the full range of their duties.

Just 48% of our respondents working in public companies were aware of these proposals, and just 44% of those working in UK companies overall. If implemented, the changes will not only put more pressure on potentially high-value targets, but will also provide claimant lawyers with more ammunition in the form of FRC reports, which can be used in claims brought against company directors.

The Criminal Finances Act

The Criminal Finances Act 2017 imposes a new criminal liability on UK and non-UK businesses that fail to prevent the facilitation of tax evasion by an 'associated person'. The new offences will come into force on 30 September 2017 with the remaining provisions of the Act also expected to come into force later this year. A particular concern for those working in professional services firms or financial institutions, the Act contains the largest expansion of UK corporate liability since the Bribery Act of 2010 (the Bribery Act), and one of the most significant overhauls of money laundering and proceeds of crime legislation in a decade.

It is already a crime to evade tax or to assist a taxpayer intent on evasion. What's new is that this legislation targets organisations that fail to prevent the crimes of those who act on their behalf. In that sense, it follows the same approach as the Bribery Act, and holds firms criminally liable where employees facilitate tax evasion by their clients. It makes businesses liable for the actions of associated persons, who are very broadly defined, and includes any persons or entities that provide a service for the business, or on its behalf (thereby encompassing foreign tax advisers, offshore accountancy firms, brokers, trustees or company director service providers, employees, agents and sub-contractors, for example).

As with the Bribery Act, the new law will also have extra-territorial effect. Non-UK businesses will be caught if they fail to prevent the facilitation of UK tax evasion (no further UK nexus is required), or in relation to foreign tax evasion if some or all of the facilitation happens in the UK, or if the foreign firms conducts business in the UK.

Charles Yorke, tax partner at Allen & Overy, says: "There is only one defence available under the Criminal Finances Act, and that is having reasonable prevention procedures in place. Businesses will need to undertake thorough risk assessments to inform the creation of prevention policies and procedures if they are to avoid criminal liabilities.

Failure by senior management to engage properly in establishing appropriate prevention procedures may weaken the ability of the company later to rely on the statutory defence if facilitation of tax evasion occurs. If the company is found guilty of the offence, the penalties include unlimited fines and confiscation orders.

Charles Yorke, tax partner at Allen & Overy, says: "There is only one defence available under the Criminal Finances Act, and that is having reasonable prevention procedures in place. Businesses will need to undertake thorough risk assessments to inform the creation of prevention policies and procedures if they are to avoid criminal liabilities."

Personal liability for errors in tax returns

In our survey, we asked respondents if they were aware of the individual personal liability that board members can incur for incorrect tax returns in some jurisdictions, such as Greece, Germany and Italy. In the UK, directors can be personally liable for unpaid national insurance contributions if the director has been fraudulent or even negligent. Only 22% of respondents to the question were aware of that exposure, which already exists and which we are aware is leading to significant claims. Even though it is the company that bears the tax, individuals can end up in court in the event of errors in tax returns.

On a closer look at the figures, only 12% of those working in UK companies who responded to the question were aware about the personal liability for incorrect tax returns, as compared with 30% of global companies. While these figures at least indicate that this issue is of greater focus in global companies (as compared with their UK counterparts), the figure of 30% still demonstrates that this is an issue which has not received much focus.

This is an area where D&O insurance generally offers little, if any, protection and such protection as is offered is often unclear. Some policies simply exclude all taxes. Others provide cover only where the company becomes insolvent and yet others offer hybrid enhanced protections whilst stepping well short of full indemnity for wilful failures to pay tax.

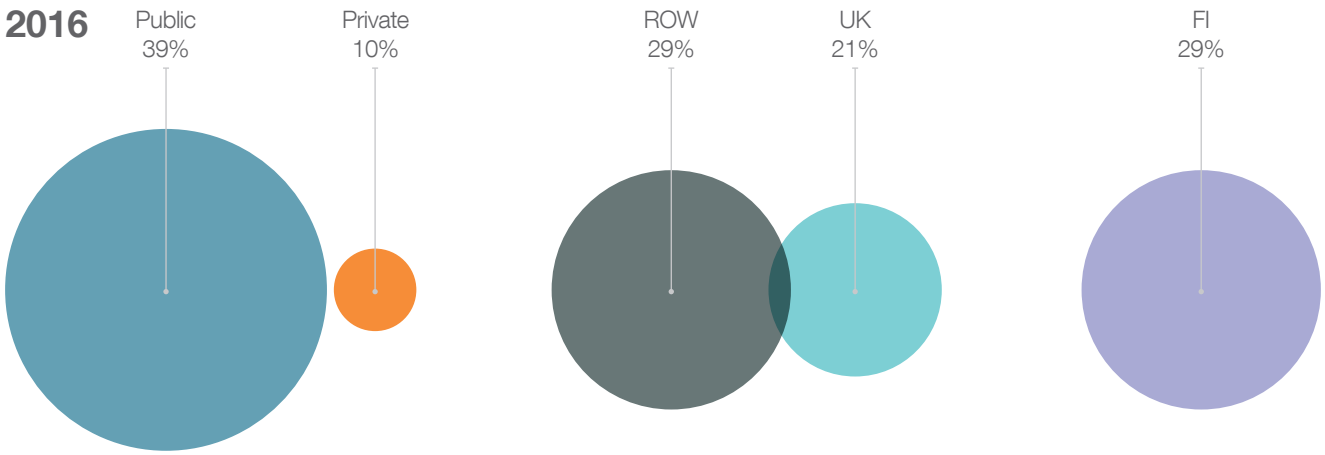
Tackling cyber and data risk

In addition to the rapidly expanding risk associated with regulatory scrutiny, two other risks continue to play heavily on the minds of directors and officers, and those relate to the risk of cyber attack and data loss. This year we were somewhat heartened to see our respondents reporting a slight fall in the number of cyber attacks: we asked whether their companies had experienced a cyber attack, or loss of data, significant enough to be brought to the attention of the board, in the last 12 months. Last year some 31% answered yes to that question, but this year the figure has dropped to 24%.

It may, however, be that the incidence of cyber attacks has not fallen, but rather the number of these incidents that are elevated to board level has reduced as companies have become more adept at dealing with what is increasingly a day-to-day threat. Alternatively, it is possible that, because there are so many cyber-attacks to deal with, boards of directors only have the bandwidth to deal with the most serious attacks. In any event, the fact that nearly one in four directors and officers has had to deal with such an incident in the last year alone is not insignificant. When we look deeper into the numbers, we see just 18% of private companies have suffered an incident as against 30% of public ones, and that 29% of predominantly UK businesses have been impacted as compared to 20% of global firms. Among our respondents in the financial services industry, only 15% reported an incident of cyber attack or data loss.

When comparing these figures to the data we received from our 2016 survey, the most stiking change is with respect to financial institutions. 35% of respondents from financial institutions last year experienced a cyber attack or loss of data significant enough to be brought to the attention of the board – 20% higher than 2017. Given that the proportion of financial institution respondents has remained flat, this statistic is very surprising, and can perhaps be explained by financial institutions focusing their attention on what is becoming one of the bigger risks that companies are currently facing.

To your knowledge, has your company experienced a cyber-attack and/or data loss significant enough to have been brought to the attention of the board in the last 12 months?



Yet while these figures may appear to deliver a positive message year-on-year, the threat of cyber attack or data loss remains an extremely significant area of concern for business leaders. After regulatory and other investigations, respondents ranked cyber attack and the risk of data loss as the next two risks that were of greatest significance to their businesses, with 81% worried about cyber attack, and 64% about the impact of a loss of data. These numbers are up considerably against a year ago, comparing to 65% and 57% respectively in our last report, and put cyber risk almost on a par with regulatory exposures. When combined – given that they are often inter-related – these two risks together are recognised as a huge exposure for business leaders.

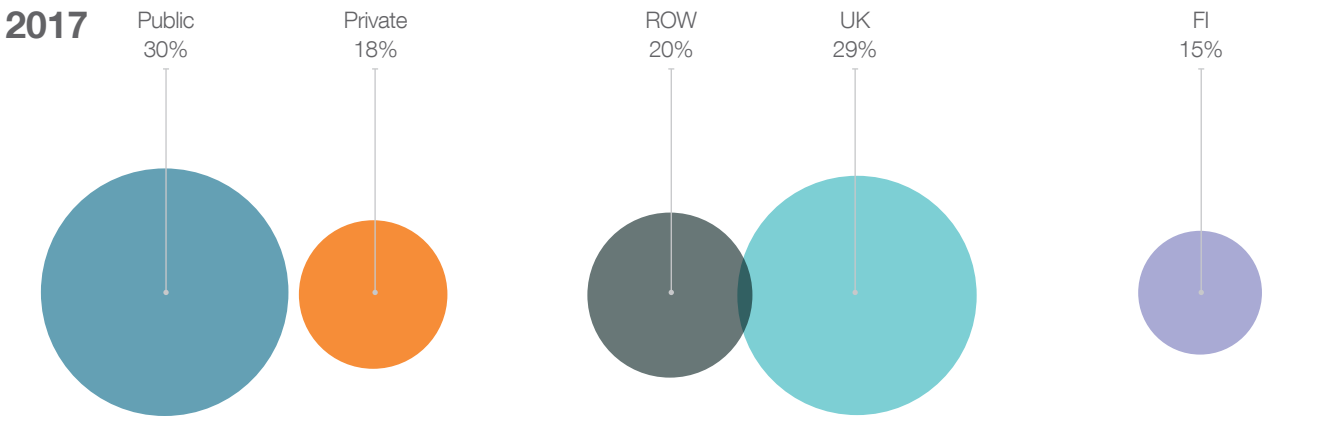
It is perhaps little surprise that the level of concern is so high, when one only has to look at recent news headlines to witness the very real and present threat that breaches of cyber security pose. In June 2017 a massive cyber attack, thought to have begun in Ukraine, spread across 60 countries and saw large companies including Mondelezand WPP receive ransom demands from the attackers. Reckitt Benckiser, the household products giant, said in July that the attack could lead to a permanent loss of revenue, and cyber attacks certainly have the potential to be catastrophic in their ability to prevent operations.

Further, in July 2017, Lloyd's of London published a report which warned that a cyber attack on a cloud service provider could result in losses of up to USD120 billion, as large as those caused by major hurricanes such as Hurricane Katrina.

Even where there is not a malicious third party involved, the potential for massive disruption to a business through IT failings should be of concern to board members: British Airways' IT systems failure being a recent example.

Regulatory bodies have been keeping a close eye on cyber security concerns. The FCA has described cyber resilience to be a 'stand out' risk area and announced its intention to undertake a "significant amount" of work in this area over the next year. On the other side of the Atlantic, the U.S. Securities and Exchange Commission has already brought several enforcement actions against registered firms for cyber security failings.

Directors and officers could find themselves personally liable for an attack against their firm if they have not complied with their extensive responsibilities relating to the prevention and management of a cyber event. Many regulatory regimes now place responsibility to implement systems and controls, and manage data usage, in the hands of managers, and they could be personally exposed to lawsuits, shareholder class actions or regulatory enforcement if they breach those fiduciary duties.



General Data Protection Regulation

The EU's General Data Protection Regulation (GDPR) was adopted on 27 April 2016 after four years of discussion, and will take effect on 25 May 2018, when it will replace the current Directive and will be directly applicable in all Member States. It contains onerous obligations, some of which will take companies time to prepare for.

The GDPR establishes a tiered approach to penalties for breaches, allowing authorities to impose fines for some infringements of up to 4% of annual worldwide turnover or EUR20 million, whichever is the higher. These increased fines are attracting the attention of executives, and yet many are still unaware of their enhanced obligations.

We asked our survey participants whether they were aware of the implications of the GDPR for their business, and a surprising 24% said that they were not; this figure rises to one in three (33%) among companies that conduct most of their business outside the UK, but encouragingly only 9% of those that work in UK companies are unaware of the new regulation's implications.

David Smith, the former deputy commissioner at the ICO, with data protection responsibility, and now a special adviser to Allen & Overy, says: "The GDPR represents a step change for businesses in their data protection obligations, not least with the introduction of mandatory reporting of data breaches to both the ICO and to affected individuals. The potential for big fines, as well as for damage to reputation, means that businesses should already be preparing for the new regime. They will have to establish priorities but doing nothing can not be an option."

The GDPR: Things you need to know

Some of the key things that executives need to know about the GDPR include:

- The GDPR has an 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, individuals in the EU.
- The GDPR places onerous accountability obligations on data controllers to demonstrate compliance.
- Data controllers and processors may need to designate a Data Protection Officers as part of their accountability programme.
- Data processors will have direct legal obligations for the first time. They will, for example, need to maintain a written record of processing activities carried out on behalf of a data controller, designate a data protection officer where required, and notify the data controller if they become aware of a personal data breach without undue delay.
- Consent must be based on a clear affirmative action, be freely given, specific, informed and unambiguous. Requests for consent should be separate from other terms, and be in clear and plain language.
- Data controllers will have obligations to document data breaches and to notify these to both the relevant data protection authority and to affected individuals.

Companies will need to consider how the new obligations apply to them, and what gaps exist between their current state of compliance and the standard that will be required next year. The sanctions for breaches are significantly higher than those under the existing regime, and as organisations are held to higher standards than previously, the risk of board members facing personal liability inthe event of litigation relating to a cyber breach or other forms of non-compliance is significantly enhanced.

In its annual report published in July, the UK's Information Commissioner's Office (ICO) revealed that in 2016/17 it had been told about more data protection breaches, and fined more companies for unlawful activities, than ever before. It expects its work to intensify next year when the GDPR gives people greater control of their own data and introduces an even more rigorous data protection regime.

Protecting directors and officers

Given the growing risks, both regulatory and otherwise, that directors and officers now face, and their increasing exposure to personal liabilities, it is perhaps little wonder that D&O policy coverage and related indemnities are becoming more of a focus of attention each year. Senior managers can take a good step towards preparing for the new regulatory focus on their conduct by taking on individual responsibility for informing themselves as to the best personal liability protection available to them through insurance and their employer's indemnity. There are, for example, some insurance products specifically geared towards the costs of legal representation in the context of the earlier stages of regulatory investigations.

Whatever an individual's priorities may be, it continues to be a stark finding of this survey that clear and easy-to-follow policy terms are a must-have when executives seek to purchase D&O policies. We asked our respondents for the fifth time what they considered to be the most significant policy coverage issues, and clear terms was once again at the top of the list. Given the much greater exposures now in play for those that are under-insured, it is understandable that individuals want to find their level of protection spelt out in plain language. On perhaps a less positive note, the fact that this concern features so prominently year on year suggests that the D&O industry needs to do more to address what is plainly an issue of some concern for directors.

Many of the other concerns were also regular features of our top five priorities: 51% of our respondents consider it to be very important that insurers' abilities to refuse claims based on non-disclosure are restricted, and 46% place considerable importance on how claims against directors and officers are claimed and settled. The coordination of the D&O policy with an employer's indemnification policy is also a priority (and is explored in more depth in the next section of this report), and so is the way in which the D&O policy, and/or company indemnification, will respond to claims in all jurisdictions.

The Insurance Act

We asked our survey participants whether the Insurance Act 2015, (the Act) which came into force in August 2016, was on their radar, and found their responses to be fairly evenly split, with 52% saying that they had not considered its impact on their D&O insurance contract. This may be a reflection of the view that, when it comes to D&O liability insurance, the Act represents something of a curate's egg. Plainly, the statutory downgrading of "basis of contract" clauses, which prior to the Act had the force of contractual warranties, is a clear win for policyholders. The position with respect to pre-inception disclosure is a little more nuanced.

Duty to make a fair presentation

The duty to make a fair presentation of the risk is probably one of the most substantial changes to be brought in by the Act. All insurance policies depend on the disclosure of material information by the party seeking insurance, which enables insurers to assess and therefore price the risk correctly. Previously, under the common law, a party seeking insurance had a pre-contractual duty of utmost good faith to disclose all relevant facts to the insurer free of any misrepresentation. The Act codified and built on this duty as a duty of fair presentation. Prospective insured parties must now disclose to the insurer all relevant risks, and every material representation must be made in good faith.

The Insurance Act

Proportionate remedies for non-disclosure

Of almost equal importance to the issue of fair presentation is the question as to what remedies are available to insurers if they wish to argue there has not been full disclosure. This is something that plainly remains on the minds of our respondents, with 51% concerned about their insurers' ability to refuse a claim based on non-disclosure – making it second only to clear policy terms as a priority for executives.

Prior to the Act, the only remedy available to insurers for non-disclosure was avoidance or rescission of the contract in its entirety. In other words, the stakes, on both sides, were very high. The position under the Act is fundamentally different.

If an insured **innocently** failed to make a fair presentation of the risk, then:

– if the insurer would not have entered into the insurance contract at all, the insurer can avoid the contract and refuse all claims, but they must return the premium; or

– if the fair presentation would have changed the insurance contract, the insurer can treat the contract as if it had been entered into on different terms.

If an insured made a **deliberate or reckless** failure to make a fair presentation of the risk then the insurer can avoid the contract, refuse all claims and keep the premium.

Impact on D&O insurance

What do all these changes mean for D&O liability insurance? Remember that parties to an insurance contract are free to vary, restrict or remove an insurance contract from the ambit of the Act should they wish to do so, but that clear language is needed, and the disadvantageous term must be brought to the insured's attention

Paradoxically perhaps, well-drafted D&O policies already contained, or should have contained, safeguards for policyholders that are arguably superior to those than the Act offers. So, for example, policies should already contain severability provisions (which ensure that the consequences of non-disclosure by one director or officer should not impact those who had no knowledge of the undisclosed facts) and 'non-avoidance' clauses, which would only allow insurers the ability to void policies in the instance of fraud.

There is a strong case to be made that this combination of contractual protections places insureds in a stronger position than they would be under the Act in the absence of such clauses. Indeed, the danger is that by introducing clauses which are designed to implement aspects of the Act, contractual protections which are already in the policy and which provide greater protection than the Act does could be watered down, or ambiguity or conflict could be created. We have already seen some cases where this has occurred, and so careful thought and attention is required.

"Well drafted D&O policies should already contain safeguards for policyholders that are arguably superior to those offered under the Act".

Investigations: divide and conquer

When an organisation is faced with a regulatory or criminal investigation, including those relating to a cyber attack or data breach, the priority is invariably to establish as quickly as possible how bad things are, seek to remedy the problem, and move on, to protect the organisation's brand and reputation. But for individuals caught up in the investigation, the priorities are different. They will wish to argue why the actions taken or not taken were reasonable in all the circumstances, to defend their positions and escape personal liability, which can include large fines, dismissal and even custodial sentences for the most serious criminal offences.

For example, the issue of third party rights of persons identified in public enforcement notices issued by the FCA has received a considerable amount of attention in recent years, with one case recently going all the way up to the Supreme Court. Under s393 of the Financial Services and Markets Act 2000 (also known as FSMA) individuals prejudicially identified, in the opinion of the FCA, in FCA warning or decision notices are entitled to third party rights. Those rights include the right to receive a copy of the notice, the right to make representations and to seek disclosure of relevant documents from the FCA. However, in this case the Supreme Court overturned the Upper Tribunal and Court of Appeal's decisions, finding instead that an individual had not been 'identified' in certain enforcement notices and therefore did not have the benefit of third party rights.

In the economic crime sphere, another way in which this divergence of interest is illustrated is in the form of Deferred Prosecution Agreements (DPAs). Although DPAs have been available in the US for a number of years, they were only introduced in the UK in 2014. A DPA is an agreement reached by a prosecutor, such as the Serious Fraud Office (SFO), and a company to suspend charges against the company that would otherwise be prosecuted, provided that the company meets certain terms. UK DPAs do not apply to individuals, however, and as confirmed in a recent speech by Ben Morgan, Joint Head of Bribery and Corruption at the SFO, the terms a company can expect to agree to when signing up to a DPA may include "terms concerning ongoing cooperation, for example in the prosecution of individuals".

Individuals identified in DPAs are not afforded the same third party protections as those identified in FCA notices, although attempts have been made to protect the interests of individuals in DPAs. For example, the SFO's second DPA with a UK SME was anonymised and certain facts held back from release pending the outcome of on-going criminal investigations. In relation to the SFO's fourth DPA, agreed earlier this year with a UK-based retailer, publication of the DPA and authorising judgment has been deferred until the trial of former senior individuals at the company has been concluded. However, arguably a different approach was taken in a DPA agreed this year with a major UK engineering company, in connection with which an investigation into individuals is still on-going. Although individuals' names were anonymised in the DPA, the judgment stated that the investigation revealed, "…the most serious breaches of criminal law in the areas of bribery and corruption (some of which implicated senior management and, on the face of it, **controlling minds of the company**".

These issues are compounded by the repeated statements by regulators in many jurisdictions to introduce personal accountability. What this means is that, if, as a price for drawing a line under a regulatory investigation, one or more individuals needs to be "sacrificed" by their employers, then that is often what will happen.

If that risk sounds exaggerated, turn again to the current edition of the U.S. Attorney's Manual issued to all DOJ attorneys: "Corporations will be eligible for cooperation credit only if they provide DOJ with all relevant facts relating to all individuals responsible for misconduct, regardless of the level of seniority… Attorneys should focus on individuals as well as corporates, taking into account issues such as accountability and deterrence – not simply ability to pay."

In other words, to obtain cooperation credit, companies are expressly required to provide the authorities with the necessary tools to pursue individuals. Seen in this context, the need to understand the traditional forms of indemnity and insurance protection and the gaps in that protection becomes even more acute, and taking control of personal coverage becomes a must.

"As confirmed in a recent speech by Ben Morgan, Joint Head of Bribery and Corruption at the SFO, the terms a company can expect to agree to when signing up to a DPA may include "terms concerning ongoing cooperation, for example in the prosecution of individuals".

Practical tips on D&O and indemnities

Indemnification and insurance products: Mind the gap

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, 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 a quarter of respondents 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 D&O	Gaps in Indemnity
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 (who 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 themselves 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 employers.

A Ten Point Checklist: the most important questions that Senior individuals may wish to consider with their employees.

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. 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?

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.


NW
N
NE
E
SE
S
300
320
340
360
20
60
80
100
120
140
160
180
200
240
260

FOR MORE INFORMATION, PLEASE CONTACT:

London

Allen & Overy LLP
One Bishops Square
London
E1 6AD
United Kingdom

Tel +44 20 3088 0000
Fax +44 20 3088 0088

GLOBAL PRESENCE

Allen & Overy is an international legal practice with approximately 5,400 people, including some 554 partners, working in 44 offices worldwide. Allen & Overy LLP or an affiliated undertaking has an office in each of:

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

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.