

*There are no tried and tested strategies for dealing with the banana skins that have shot to the top of reinsurers' risk registers – cyber risk, change management and political upheaval. How can you get to grips with these highly unpredictable and disruptive exposures?*

# ***Uncharted waters: Tackling reinsurers' riskiest exposures***







---

**Contents**

Introduction: New forms of risk require new approaches	4
Taking cyber risk out of the too difficult pile	8
Managing at the speed of change	14
Dealing with political upheaval	17
Make or break	22

# **Introduction:**

## New forms of risk require new approaches

*Welcome to Uncharted waters: Tackling reinsurers' riskiest exposures. The report explores the most serious risk concerns among the reinsurers that took part in the Insurance Banana Skins Survey 2017<sup>1</sup>, and how to deal with them.*



<sup>1</sup> The Insurance Banana Skins Survey 2017 draws on the perspectives of 836 practitioners and close observers of the industry in 52 countries, of which 58 were reinsurers (<http://www.pwc.com/gx/en/industries/financial-services/insurance/insurance-banana-skins-2017.html>). The survey is the latest in the CSFI's long-running Banana Skins series on financial risk. The report is prepared by the CSFI, which is solely responsible for the editorial content, with support from PwC.

Insurance Banana Skins is a unique survey of the issues at the top of the industry's risk register and how these perceptions change over time. The biennial report is produced by the The Centre for the Study of Financial Innovation (CFSI) in association with PwC.

What's most striking about the latest set of results is how far and how fast the risk landscape is shifting. Having for many years been dominated by the familiar headaches of solvency regulation and a challenging market environment, the risks that now cause the most sleepless nights are rooted in the shock and uncertainty of the new.

At number one is cyber risk, reflecting both the anxieties of underwriting a risk that's constantly shifting and the rising threat to reinsurers themselves. Far from being just a technology risk, cyber is now a huge reputational and systemic concern.

At number two is the industry's ability to address a formidable agenda of new technology and shifting customer and conduct expectations, along with the associated pressure on service, performance and costs. Signs of the upheaval are all around us, from new forms of underwriting and risk transfer, to increased automation and inroads from InsurTech right along the value chain. And even more disruption is coming up on the horizon in areas ranging from artificial intelligence (AI) to driverless cars.

We also focus on what the Banana Skins survey describes as 'political interference' on account of its rapid rise up the risk rankings and particular relevance to prominent reinsurance centres, notably the UK and Bermuda. As a global industry, reinsurance faces considerable challenges from the political developments, changes in trading arrangements and the shift towards more nationalistic rather than global approaches. Our analysis of the implications looks in particular at the implications of Brexit and an uncertain US tax agenda.

## **Threats and opportunities**

What cuts across all cyber risk, change management and recent political upheaval is the limited experience in dealing with them, and hence the need for new thinking and fresh approaches to risk management. The strategic nature of these risks mean that the response will determine the success and even survival of market participants. At the same time, they present opportunities to capture valuable new sources of revenue and lead innovation in a rapidly evolving global marketplace.

## **Down but by no means out**

A notable faller in the list of risk concerns is regulation, having been in reinsurers' top three in the previous Banana Skins reports in 2013 and 2015<sup>2</sup>. This is largely because recent regulatory changes predominantly relating to solvency are settling into business as usual (e.g. Solvency II), though the cost and complication of regulation continue to be a concern, including for example, developments in conduct and intermediary regulation<sup>3</sup>. Linked to this, recent geopolitical developments, including Brexit and changes in trading arrangements, create a range of regulatory challenges in key areas including market access and cross-border supervision. We look at these impacts as part of our focus on the three leading risk concerns.

---

*Signs of the upheaval are all around us, from new forms of underwriting and risk transfer, to increased automation and inroads from InsurTech right along the value chain. And even more disruption is coming up on the horizon in areas ranging from artificial intelligence (AI) to driverless cars.*

---

2 Insurance Banana Skins 2013 and 2015 (<http://www.cfsi.org/insurance-banana-skins/>)

3 IAIS Consultation on ICPs 18 and 19 (Intermediaries and Conduct of business) <https://www.iaisweb.org/page/consultations/current-consultations/revision-of-icps-12-18-19-and-24>



## Top risks

### Reinsurers' Banana Skins 2017

(2015 ranking in brackets)

1	Cyber risk	(3)
2	Change management	(-)
3	Investment performance	(8)
4	Macro-economy	(10)
5	Technology	(-)
6	Competition	(-)
7	Political interference	(-)
8	Interest rates	(4)
9	Regulation	(2)
10	Cost reduction	(-)

(-) denotes new to top ten

### Insurers' (all segments) Banana Skins 2017

(2015 ranking in brackets)

1	Change management	(6)
2	Cyber risk	(4)
3	Technology	(-)
4	Interest rates	(3)
5	Investment performance	(5)
6	Regulation	(1)
7	Macro-economy	(2)
8	Competition	(-)
9	Human talent	(-)
10	Guaranteed products	(7)



## Top risks by country or region (all segments)

### Europe

- 1 Interest rates
- 2 Cyber risk
- 3 Change management
- 4 Technology
- 5 Guaranteed products

### North America

- 1 Change management
- 2 Cyber risk
- 3 Technology
- 4 Human talent
- 5 Competition

### Asia Pacific

- 1 Change management
- 2 Technology
- 3 Cyber risk
- 4 Investment performance
- 5 Human talent

### Bermuda

- 1 Cyber risk
- 2 Regulation
- 3 Political interference

### Germany

- 1 Interest rates
- 2 Guaranteed products
- 3 Change management

### Switzerland

- 1 Interest rates
- 2 Change management
- 3 Investment performance

### UK

- 1 Cyber risk
- 2 Interest rates
- 3 Technology

### US

- 1 Cyber risk
- 2 Change management
- 3 Technology

# Taking cyber risk out of the too difficult pile

*A collaborative approach that brings together active threat intelligence and technical underwriting rigour holds the key to realising the full commercial potential of cyber risk.*

If risks are generally measured by their frequency and severity, then cyber adds a third and highly disruptive dimension – the capacity to confound.

This is a risk that's constantly morphing as cybercriminals probe for vulnerabilities in an increasingly digitised and interconnected global economy. Behind the scenes, an ever more sophisticated game of 'cat and mouse' is being played out between perpetrators and security experts.

And cyber is far from just a systems risk. High profile breaches such as May's WannaCry ransomware attacks highlight the extent to which cyber is also a severe reputational and business interruption risk – it can take just one incident to bring organisations to a halt and trigger a board-level crisis. In turn, a spate of less well-publicised near misses, most notably 2016's Operation Cloud Hopper, underline the potential systemic threat posed by such attacks, and the immense ambition, ingenuity and reach of the perpetrators.

## **Unfulfilled potential**

In an otherwise soft and slow growth market, safeguarding businesses against these attacks offers a sizeable opportunity for reinsurers across the direct cover, reinsurance, retrocession and risk advisory areas of business. Reinsurers'

technical underwriting prowess and experience of managing diffuse accumulations of risk give them an important edge, not just in relation to standalone cyber cover, but also in dealing with 'silent' exposures within broader policies such as general liability (GL), directors & officers (D&O) and marine, aviation and transport (MAT).

Based on the potential demand for cyber insurance and the industry's capacity to meet it, PwC's 2015 estimates indicated that the market for standalone cyber insurance could more than double to reach \$7.5 billion in annual premiums by the end of the decade<sup>4</sup>. Other market commentators have suggested that values could rise to as high as \$20bn by 2025<sup>5</sup>.

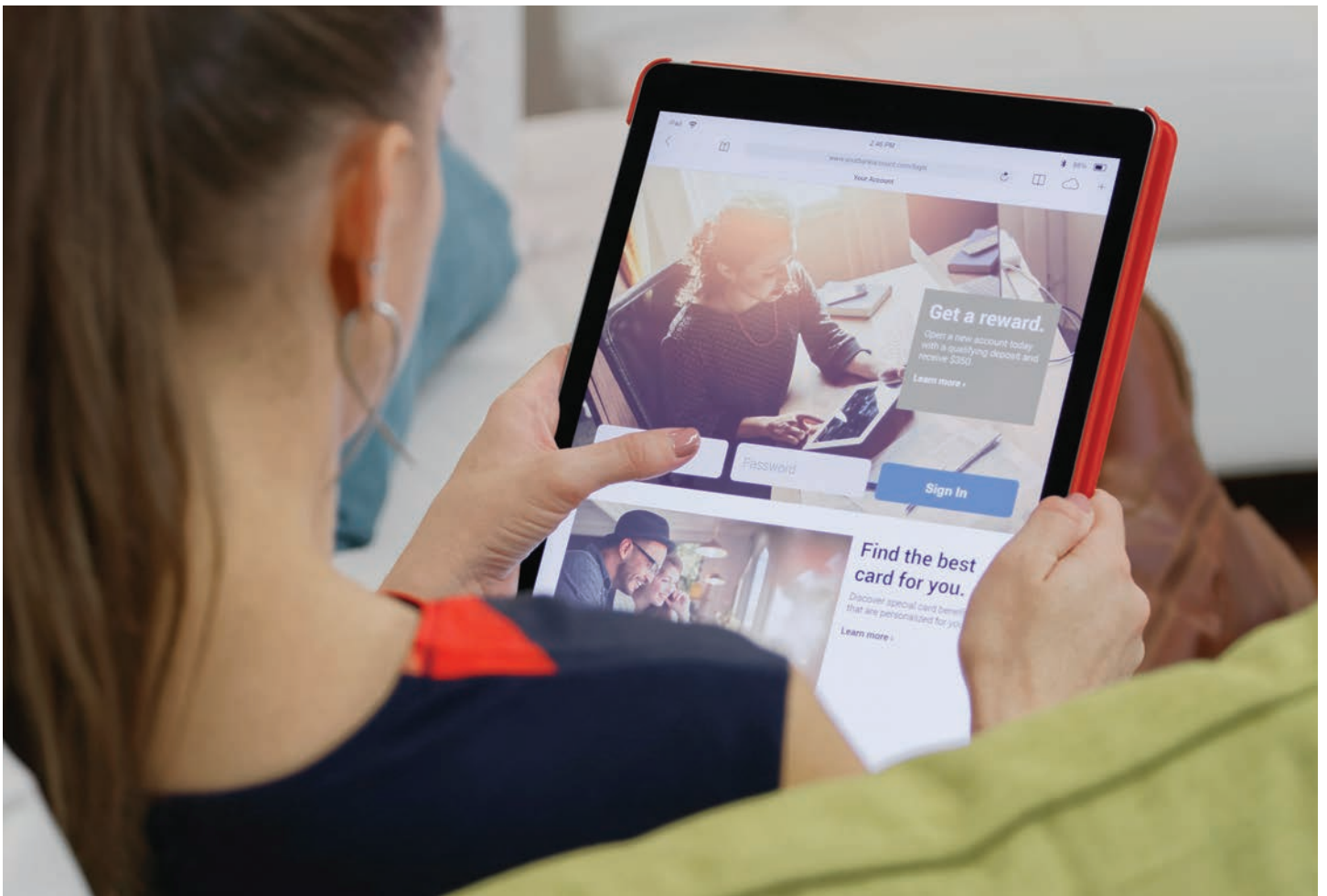
However, actual growth in the cyber insurance market has so far been slower than expected given the scale of the threat – premium volumes reached an estimated \$3.5 billion in 2016<sup>6</sup>. With the US accounting for \$3 billion of the \$3.5 billion in global revenues, the potential for further penetration in other parts of the world is clear. Yet even in the US, less than 40% of businesses have specific cyber insurance cover. Worldwide, the scale of underinsurance is especially marked among small and medium sized enterprises (SMEs).

4 'Insurance 2020 and beyond: Reaping the dividends of cyber resilience', PwC, 2015 (<http://www.pwc.com/gx/en/industries/financial-services/insurance/publications/insurance-2020-cyber.html>)

5 'A Guide to Cyber Risk Managing the Impact of Increasing Interconnectivity', Allianz Global Corporate & Specialty, <http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf>

6 'Supporting an effective cyber insurance market', OECD report for the G7 presidency, May 2017 (<http://www.oecd.org/internet/supporting-an-effective-cyber-insurance-market.htm>)





## **Businesses want more protection than they're getting**

Why is take-up of cyber insurance still so low? Capacity isn't an issue – PwC's analysis suggests that there is a lot more of it than demand at present as insurers and reinsurers actively target the cyber market, albeit certain industry sectors are largely avoided or subject to penal rates. Some observers argue that it will take a major data breach or operational breakdown for cyber insurance demand to really take off across the board. Yet, we know from our cyber security work with a wide range of corporations that many executives who are fully aware of the loss potential are nonetheless reluctant to buy cyber cover. This is largely because the generally restrictive coverage and limits on offer are seen as curtailing the level of protection they gain.

With so much uncertainty surrounding cyber risk and little historical data to go on, many insurers and reinsurers are wary of raising the cyber cover limits they're willing to offer. One of the reasons why cyber risk tops reinsurers' list of banana skins is their concern over the scale of the potential losses they face from unforeseen accumulations of exposure, which is heightened by the systemic threats and uncertainty over liabilities. Looking at the potential impact of a major cyber attack on

the insurance market as a whole, recent scenario analysis carried out by Lloyd's estimated that the average insurance losses from its mass software vulnerability scenario could be between \$762 million to \$2.1 billion and between \$620 million to \$8.1 billion for its cloud service disruption scenario.<sup>7</sup>

Yet, the market won't achieve its growth potential unless underwriters are prepared to offer increased protection for their clients, while at the same time finding ways to lay off or diversify some of the increased accumulation of risk. And it isn't just higher limits that businesses want, but also coverage that reaches beyond the often narrow focus on systems and data to embrace the full cost on the business from lost revenue due to the disruption. They're also looking for ways to protect their reputation by preventing attacks and, if they are hit, to minimise the damage by helping them to get back up and running as quickly as possible.

## **Taking the initiative**

So how can your business overcome the barriers holding back growth in the cyber insurance and reinsurance market and capitalise on its full potential?

<sup>7</sup> Lloyd's media release, 17 July 2017 (<https://www.lloyds.com/news-and-insight/press-centre/press-releases/2017/07/cyber-attack-report>)

### 1 Partner

One of the key questions facing the market is whether underwriters or specialist digital security companies are best placed to evaluate and make underwriting decisions around cyber risks. In our experience, a close working partnership between both parties is needed – neither can do it on their own.

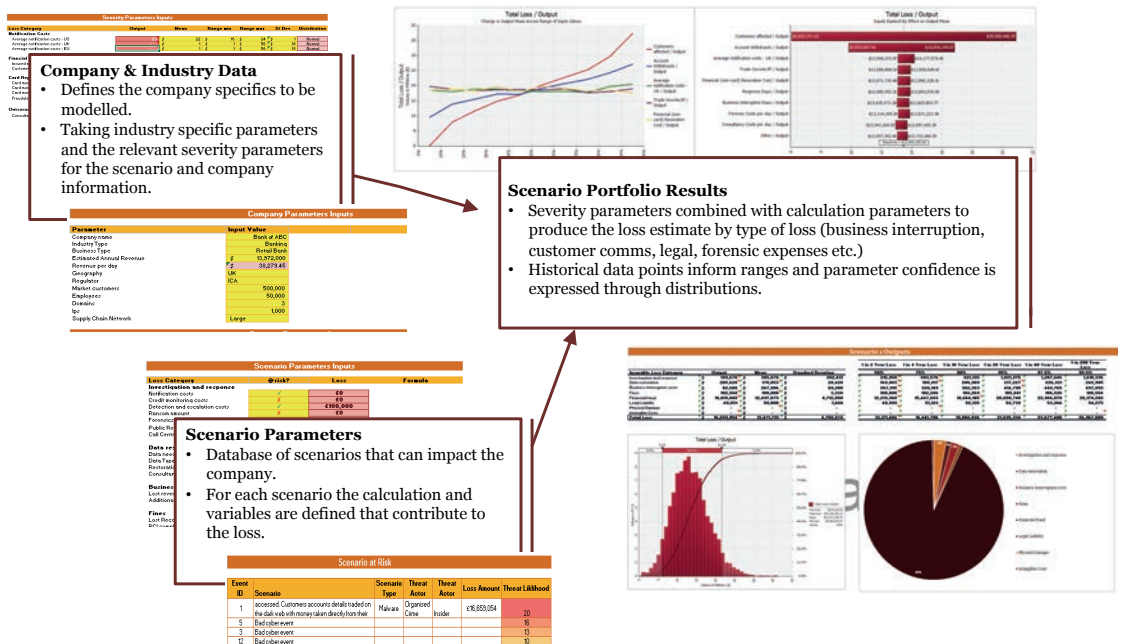
Digital security companies can provide the up-to-date threat intelligence, insights into potential attackers and expert evaluation of the level of protection within the insured’s business. As an insurer and reinsurer of cyber exposures, your key role in selecting and pricing the risks is a clear understanding of the client’s business and its risk management capabilities from a technical underwriting perspective.

For corporate clients, this includes evaluating their IT dependency, supply chain risks, and the most prized and sensitive data assets (‘crown jewels’). It also includes rating the training provided to employees, as a surprisingly high proportion of breaches can be traced back to phishing and less technology-focused approaches. This all-round evaluation can form the basis for assessing business interruption costs, both directly and through the potential for third party claims from key customers and suppliers (Figure 1 illustrates an example of how different data and analysis can be brought together within the loss estimates). For (re)insurers, this cyber risk intelligence is further applied to assess accumulations from a systemic cyber event, both in their standalone cover and broader policies.

For (re)insurers, this cyber risk intelligence is further applied to assess accumulations from a systemic cyber event, both in their standalone cover and broader policies.

Figure 1

## Cyber loss quantification framework for insurance portfolios



Source: PwC

## 2 Get proactive

This more informed risk and scenario evaluation can not only sharpen underwriting, but also develop loss prevention and mitigation services as a 'value-added' offering to your clients.

It's important to work with both insurers and corporate clients to gain a better understanding of their vulnerabilities and how they can strengthen safeguards. With the risks better understood and controlled, it would be possible to offer higher limits. You could also offer favourable pricing for better protected clients. And because you have a better understanding of your clients' risks, you're in a better position to control your own exposures and risk profile.

## 3 Sharpening assessments of systemic scenarios

Historical data on cyber losses is limited. However, analysis of the many near misses and thorough monitoring and evaluation of the latest threat intelligence can help to gauge vulnerabilities, assess exposures and develop more informed scenario assessments. An important part of this evaluation is the ability to capture exposures and any mitigants to these across entities and lines of business, and then bring this together to test a (re)insured's vulnerability and response to a cyber event. This is especially critical on the silent side where a single event could trigger very material losses across multiple entities, lines of business and geographical boundaries.

## 4 Target your market – standalone policy or additional peril?

Another key strategic question is whether to focus on standalone cover or include cyber risk as an additional peril within broader policies.

Adding cyber cover to policies targeted at SMEs would enhance the value of the insurance and provide a useful distribution opportunity within this largely untapped market segment for cyber protection. There are direct openings for reinsurers here. There are also opportunities to work with insurers to help them understand the risks and accumulations on their books, and hence gain greater confidence in increasing the availability of cover and level of protection.

At the other end of the spectrum, the heightened scale of the risks facing large corporates and generally bespoke nature of their IT systems call for standalone cyber cover.

In many ways, the most challenging market segment lies between the SMEs and the large corporates. The threats and losses they face, which are exacerbated by their less sophisticated cyber defences, call for standalone cyber insurance. However, it may be uneconomic to offer the level of bespoke evaluation, advice and cover offered to bigger groups. The answer is likely to be an industry focused approach, which combines threat intelligence with knowledge of the business dynamics within particular sectors gained from other parts of your underwriting portfolio. The threats and vulnerabilities vary from sector to sector, though our analysis highlights the extent to which cybercriminals are now spreading their net beyond what have traditionally been seen as 'high-profile' sectors – such as defence, energy, pharmaceuticals and financial services – to target new industries and organisations.

---

*Adding cyber cover to policies targeted at SMEs would enhance the value of the insurance and provide a useful distribution opportunity within this largely untapped market segment for cyber protection.*

**5 Protect your own ‘crown jewels’**

As more and more insurance and reinsurance business moves over to digital channels, the industry’s own vulnerabilities to hacking, fraud and data compromise continue to mount (see Figure 2). The risk is heightened by the volume of medical, financial and other sensitive policyholder information held by insurers, which if compromised would lead to a loss of trust that would be extremely difficult to restore. It would be difficult to sustain the credibility

of risk evaluation and advice if your business suffered a preventable breach. Cyber has also been identified by regulators as a key risk area, with the International Association of Insurance Supervisors (IAIS) encouraging supervisors to consider cyber resilience as part of their prudential evaluations of governance and risk management, as well as customer conduct, safeguards<sup>8</sup>.

**Figure 2: Cyber Security Context for Financial Services – Increasing balance between internal and external challenges, threats and demands**



8 IAIS Issues Paper on Cyber Risk to the Insurance Sector, 2016, (<https://www.iaisweb.org/page/supervisory-material/issues-papers>), Issues Paper on Conduct of Business Risk and its Management, 2015 (<https://www.iaisweb.org/page/consultations/closed-consultations/issues-paper-on-conduct-of-business-risk-and-its-management>)

The proactive risk management approach used in your cyber underwriting would also greatly strengthen the protection of your own systems, data assets and brand reputation. In addition, it's important to raise awareness throughout your organisation and build cyber into your enterprise risk management, rather than just leaving security to IT. Collaboration with industry peers is vital, not only in sharing threat intelligence and co-ordinating responses, but also in pooling expert resources at a time when dedicated cyber security talent is in short supply.

### ***Ready for take-off, ripe for disruption***

The cyber insurance market has close parallels with catastrophe cover. Since the wake-up call of Hurricane Andrew in 1992, investment in modelling and analytics has enabled the industry to insure most natural catastrophes. As well as developing the analytical and underwriting approaches needed to confidently offer the cyber cover clients want, insurers and reinsurers have to find ways to manage the systemic risks opened up by these escalating cyber threats.

The prize is the ability to capture revenues that could eventually equal or even exceed catastrophe premium values. However, there are plenty of disruptors looking to move into this high margin market. They include digital security companies and, of course, alternative capital, although insurance-linked securities (ILS) with a cyber event trigger are rare at this stage. Technology giants are also unlikely to miss the opportunity. Indeed, they may even be forced by shareholders to provide some form of cover or cyber risk prevention services should their business models be threatened by falling consumer confidence in the global digital economy. This hasn't happened yet, but if major losses emerge, the possibility would increase.



# Managing at the speed of change

*Change is coming at reinsurers at a phenomenal pace. How can you get innovation and its implementation in your business up to speed?*

While new regulation has been the source of considerable upheaval in recent years, the accelerating developments in technology and customer expectations could have an even bigger impact on business models, the capabilities needed to compete, and even what we mean by insurance and reinsurance.

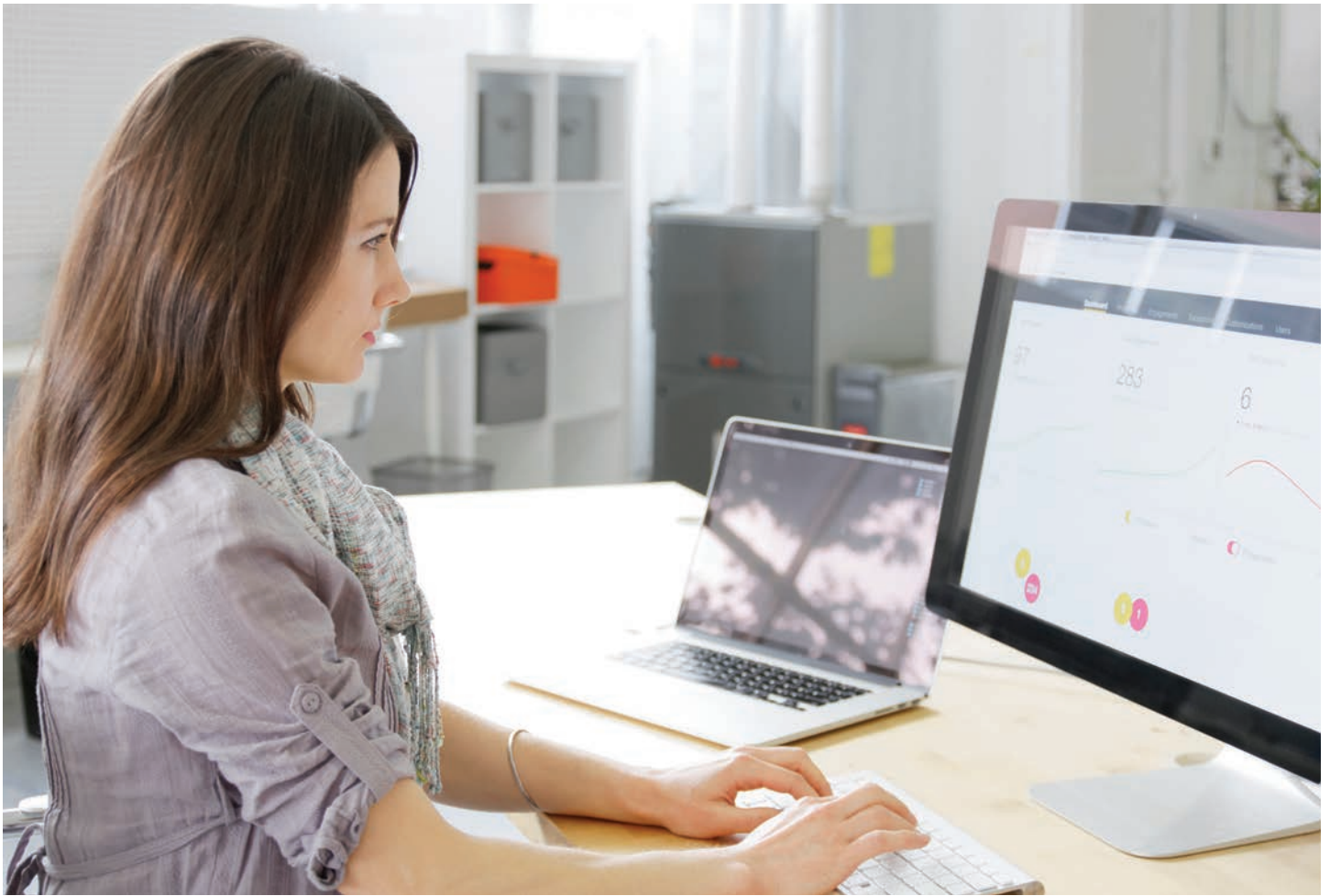
## ***Ever increasing customer demands***

Customers want to access cover and to be able to settle claims at the push of a button, with their expectations shaped by their digital retail experiences – the longer it takes, the more likely you are to lose them. The capabilities to meet these expectations are there for less complex business lines – developments in robotic process automation (RPA) mean that customers can go from policy search, quotation and origination of motor cover through to claims notification and settlement without directly interacting with a single human being, for example. The benefits include being able to pay out routine claims in a matter of minutes, while handlers have more time to focus on complicated cases. The challenge for businesses struggling to get by with antiquated legacy systems is how to compete with much faster and lower cost rivals – both InsurTech players and established businesses.

## ***New techniques***

In turn, developments in analytics, sensors, AI and internet of things (IOT) technologies are pushing back the borders of customer profiling and risk evaluation. This includes being able to move from anticipating losses (predictive analytics) to proactively shaping the outcome (prescriptive analytics) in areas such as reduced road accident rates or improved catastrophe resilience. The potential shifts in business model include moving from annual renewal to a full-time service and advisory model. The challenge is determining where to focus investment and development when there are so many innovations coming through, and start-ups and traditional vendors all vying for your attention. With your business now awash with data, much of it raw and unstructured, it's also difficult to cut through to the insights that count.

And potentially even bigger changes lie ahead. These include driverless cars and other forms of autonomous transport. In the former case, this will shift the focus of motor cover from the driver to a vehicle warranty (including product liability coverage), the competitive impact of which could be heightened if manufacturers and/or technology companies include insurance as part of a comprehensive mobility service. The combination of more precise tech-enabled risk evaluation and capital searching for yield could also extend the scope of ILS.



### **Struggling to keep up**

The difficulties of keeping pace with market transformation have propelled change management to number two on reinsurers' list of risk concerns, having not even featured in the top ten in 2015. While scale has always conferred considerable competitive advantages within the reinsurance market, it can make it harder to move with the nimbleness required in such a rapidly evolving market. Industry leaders' recognition of the scale of the shake-up is further underlined by the findings of PwC's latest CEO Survey, which reveals that insurance has now overtaken entertainment & media as the most disrupted sector in the global economy<sup>9</sup>.

### **Regulators involved too**

It's not just (re)insurers that are pre-occupied by change; regulators are also monitoring the developments and the challenges they create as a top supervisory priority. Common concerns include the sustainability of legacy systems. Regulators are also looking closely at the impact of change on customers and service. Not only must insurers and intermediaries treat customers fairly, they must also provide value across the distribution chain; the increasing use of technology and data puts a whole new lens on customer risk in the regulators' eyes, while also

challenging the customer value of traditional models. It's no surprise that both the Financial Stability Board and the IAIS have commented on conduct standards<sup>10</sup>, with the IAIS already having issued an Insurance Core Principle (19) with a recent consultation paper update<sup>11</sup>.

### **Up to speed**

So how can your business move at the speed of change?

#### **1 Embracing experimentation**

Incremental innovation and marginal change won't be enough to sustain profitability and growth in this disrupted marketplace. It's therefore vital that boards and business teams embrace experimentation and bring innovation in from the fringes of the business and into the mainstream.

Embracing experimentation can be a difficult cultural hurdle in an industry that's accustomed to big decisions in areas such as systems implementation and product development. But innovation requires lots of little decisions, some good and others to learn from.

Alongside a change of mind-set, this calls for a shift in decision making processes, performance management and incentives.

9 Based on the percentage of CEOs who are extremely concerned about the threats to their growth prospects from over-regulation, the speed of technological change, changing customer behaviour and competition from new market entrants. Source: 'Embracing possibility, boosting innovation: Key findings in the insurance industry from PwC's 20th CEO Survey' (<http://www.pwc.com/gx/en/ceo-survey/2017/industries/pwc-ceo-20th-survey-report-2017-insurance.pdf>)

10 FSB paper on the Financial Stability Implications From Fintech: <http://www.fsb.org/wp-content/uploads/R270617.pdf>

11 IAIS CP ICP 19 Revised for Public Consultation: <http://www.iaisweb.org/page/consultations/current-consultations/revision-of-icps-12-18-19-and-24/file/67206/icp-19-revised-for-public-consultation>

**More than half of the insurers taking part in PwC's 2017 Global FinTech Survey have now put InsurTech at the heart of their strategies and 45% are partnering with innovators, up from 28% last year. Partnership provides access to innovation without the fixed costs of in-house development.**

## **2 Tracking change**

Many of the front-runners have created a dedicated innovation team to keep track of technological developments, identify threats and opportunities, and work with the board and business teams to judge how to respond. How could these innovations support your strategy? What operational 'pain points' could they help to address? Armed with these insights, you can begin to develop an enterprise innovation model that looks at where to target investment and what talent and connections with innovators are needed to take advantage of the latest developments.

## **3 Promoting collaboration**

Cutting edge customer interaction and data analytics have enabled InsurTech businesses to set the pace in the marketplace. While established players have in the past tended to regard InsurTech as a disruptive threat<sup>12</sup>, our latest research shows that they're embracing the possibilities of collaboration<sup>13</sup>. More than half of the insurers taking part in PwC's 2017 Global FinTech Survey have now put InsurTech at the heart of their strategies and 45% are partnering with innovators, up from 28% last year. Partnership provides access to innovation without the fixed costs of in-house development. In our experience, the reinsurers that are making the most of the potential aren't just supporting InsurTech development through funding, but also sharing insights from their market experience and providing an incubator and testing ground for new ideas and ventures.

## **4 Rethinking talent**

Talent is just as important as technology in keeping pace with change as you look to bring together a workforce that's agile, creative and able to strengthen customer insight. Diversity is regarded by many CEOs as a top issue, not only to avoid group think and improve innovation, but to create an environment that reflects the customer base and supports business growth, engagement and service.

Broader skills sets are needed – cyber security expertise is a clear case in point. As AI and RPA become ever more important, demand for programmers, data scientists and robotics engineers is also set to increase. It's therefore important to seek out new sources of talent, many of which will come from beyond the (re) insurance industry. The way you deploy and manage talent is also set to change as working alongside AI becomes routine.

## **Vision for a market that's opening up**

Change is disorientating, but it can also be liberating. Technology and shifting customer demand open up opportunities to carve out new value propositions and reinvigorate growth. The reinsurers out in front are embracing disruption and the curiosity and creativity that come with it.

12 'Opportunities await: How InsurTech is reshaping insurance' drew on interviews with executives involved in digital and technological transformation from 79 insurers worldwide (<http://www.pwc.com/gx/en/industries/financial-services/fintech-survey/insurtech.html>).

13 'Insurance's new normal: Driving innovation' draws on interviews with executives involved in digital and technological transformation from 189 insurance companies from around the globe (<http://www.pwc.com/gx/en/industries/financial-services/fintech-survey/report/insurance.html>).



# Dealing with political upheaval

*As political developments lead to re-negotiation of international ties with never before challenges to globalisation, the (re)insurance sector faces having to address possible shifts in business arrangements, including where you operate and how you structure your organisation.*

Reinsurance is a global sector operating in a world that's facing a significant, albeit still partial, retreat from globalisation. The fallout can already be seen in the US' withdrawal from the Trans-Pacific Partnership and the UK's vote to leave the EU. In their place we're seeing a return to an age of bi-lateral ties and bespoke sector-by-sector trade agreements as companies, governments and trading blocs shop around for the best deal and jostle for favoured status.

Reinsurers' concerns over the impact of 'political interference' is highlighted by its move up to number seven on the list of banana skins. In some markets, notably Bermuda, it's even higher (number three) among insurers and reinsurers. The anxieties are further highlighted in PwC's CEO Survey – 60% of (re)insurers believe that it's becoming harder to balance competing in an open global marketplace with trends toward more protectionist national policies<sup>14</sup>.

## **Brexit impacts for (re)insurance**

London is a major insurance and reinsurance centre. While its global status won't change, Brexit opens up complex considerations. And with businesses from around the world coming to London to access global and specialist risks, the implications of Brexit will reach beyond the UK and EU.

Key considerations include whether the passporting rights, which allow UK-based (re)insurers, brokers and agents to underwrite and intermediate business anywhere in the EU and vice-versa, will continue. If not, what are going to be put in their place?

The UK could eventually seek 'equivalence' under Solvency II just as Switzerland and Bermuda have done, or an alternative form of 'mutual recognition', perhaps along the lines of the US Covered Agreement. Both approaches would allow reinsurers operating from the UK to serve EU clients without penalties, and avoid complex group supervision arrangements for (re)insurance groups. However, a wider bilateral arrangement would be required to afford full market access for both UK and EU (re)insurers akin to passporting, and to ensure a level playing field.

For brokers and intermediaries, the fact there is no equivalence or third country framework within the Insurance Distribution Directive (IDD), which is due to be implemented in 2018, means that mutual access would also require a bespoke agreement.

Without a bilateral arrangement providing for "passport or equivalence type" outcomes, it will be necessary for businesses operating between the UK and EU to consider options for restructuring and relocation. These include setting up new entities to underwrite and distribute products and services within the EU and UK, and ensuring compliant arrangements for business flowing between UK and EU.

<sup>14</sup> 'Embracing possibility, boosting innovation: Key findings in the insurance industry from PwC's 20th CEO Survey' (<http://www.pwc.com/gx/en/ceo-survey/2017/industries/pwc-ceo-20th-survey-report-2017-insurance.pdf>)

***It may be some time before there is clarity over the future trading arrangements between the UK, EU and international markets worldwide. A number of issues are at stake depending on what's eventually agreed, and the timing of this, together with any transitional arrangement:***

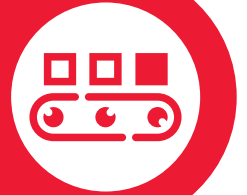
### **1 Cost**

If separate subsidiaries are needed for UK and EU operations, this would inevitably lead to higher capital and compliance costs, in particular for (re)insurers under Solvency II who have benefitted from solvency capital diversification benefits through passport structures. The implementation of the IDD, which will affect both (re)insurers and intermediaries, will increase compliance costs, more so under Brexit given the complexities of structures and business flows. Brexit could also create potential inefficiencies for reinsurance, depending on the outcome on equivalence.



### **2 Capacity**

The additional costs and inefficiencies are leading some companies to consider the sustainability of the business and to discontinue certain lines. Divestment is likely to accelerate the consolidation of some lines of business. As the market shifts to adapt to the new environment and structures, capacity will flex and require careful management.



### **3 Complexity**

Setting up new subsidiaries will introduce governance and operational complexities, for example through matrix structures and outsourcing arrangements, and, for (re)insurers, heighten the complications of Solvency II group supervision for groups with UK and EU operations.



### **4 Competition**

The structural changes resulting from Brexit have potential implications for the broader competitive landscape, both within the EU and UK as a result of inefficiencies, and beyond, with the UK seeking bilateral ties with non-EU jurisdictions. There is a risk that global regulatory developments will become more national in their implementation, which would make convergence with Solvency II and a consensus for ComFrame<sup>15</sup> look challenging. Collectively, these open up the potential for competitive impacts between local, regional and global players.



### **5 Contract certainty**

Differences in the regulated activities and licensing requirements within EU member states, coupled with the time needed to move portfolios, could affect the ability to legally settle claims. This is a key issue which also potentially impacts firms in run-off, and some may require new EU/UK authorised entities to fulfil existing obligations post-Brexit. Multi-year and long tail policies require particular attention.



<sup>15</sup> The IAIS-led Common Framework (ComFrame) aims to provide the basis for global convergence of the regulatory and supervisory measures for internationally active insurance groups (<https://www.iaisweb.org/page/supervisory-material/common-framework>).

## **How Brexit affects your business**

The impact of Brexit differs according to the particular business, operating and finance model in place, as well as the wider group context – there is therefore no one-size-fits-all solution:

- **For UK (re)insurers**, the focus to date has been on determining the most appropriate structure and EU domicile if the UK leaves the EU Single Market, and mutual passporting rights no longer exist. Likewise inwards EU passporters into the UK need to carefully consider their structure and regulatory status in the UK.
- **For London Market firms** (UK, EU and internationally based), it's also important to look at how the operating ecosystem and business flows may change, both as part of the settlement between the UK and EU, and any subsequent free trade agreements (FTA) between the UK and markets around the world.
- **For businesses benefiting from equivalence arrangements**, considering the terms of these agreements and any standalone FTAs and memorandums of understanding that might come into play is key.
- **For brokers and intermediaries**, the structural impact depends on distribution models and whether the firm already has separate subsidiaries within the UK and EU – many larger brokers do, but others don't.

For all firms, it's important to map business flows between the UK and EU to gauge any restrictions, the potential need for an EU entity and the compliance implications, with Solvency II considerations and the impact of the IDD forming a crucial part of this assessment. A particular focus under IDD will be business involving multiple intermediaries, such as some cover holder arrangements, and the new product oversight requirements for insurers and intermediaries who manufacture products. For commercial lines and reinsurance business, contemplating how business flows between broker networks will be key.

More broadly, the new IDD regime will have significant implications for insurers and intermediaries, as well as greater responsibilities for supervisors. The timing of its implementation in 2018, coupled with guidelines and technical advice continuing to be issued by European Insurance and Occupational Pensions Authority (EIOPA), and member states consulting on their implementation, adds further complexity to firms navigating Brexit.

## Planning for Brexit

The eventual outcome of the Brexit negotiations remains uncertain. However, time is of the essence and there are a number of important considerations for businesses to take into account in preparing contingency plans:

1

### Evaluate the potential impact

- Brexit scenario analysis – a full impact analysis will enable you to judge what the different post-Brexit scenarios mean for your business and to develop a Brexit strategy and contingency plans (outcome and timing).
- Review organisational impact – it's important to consider the breadth of your business, operating and finance model. Key questions to ask include: Where are your most important clients located? What access rights do you currently use? How does business flow to you? How will Brexit impact your systems, people and data? What are the capital, reinsurance and rating impacts?

2

### Determine the Brexit objectives and overall strategy

- Consider the wider strategic landscape – the key is to consider Brexit alongside wider business developments and change programmes, and to use these changes as an opportunity for re-evaluating target markets and business strategy, as well as modernising the structure and operations of your business.
- Establish design criteria and priorities for Brexit – it's important to define the priorities for your post-Brexit end-state. For example, if you're considering establishing an EU regulated entity, determine your domicile criteria (for example, tax treaties, supervisory style, infrastructure, language etc.), target efficiencies and preferred operating model, from both a local and wider group perspective.

3

### Evaluate Brexit options, define structure and transition mechanism

- Identify options and assess against defined criteria – key considerations include your legal entity structure and domicile options, assessing regulatory perimeter issues, transaction flow options, and approaches to managing contract certainty risks, as well as variations in member state requirements.
- Review transition approaches and confirm their feasibility and cost benefit – considerations include possible merger options (also the merits of merging to establish a 'Societas Europaea' – European limited company), as well as portfolio transfers, and developing transition step plans dealing with accounting, regulatory and tax.

4

### Build out your Brexit end-state

- Implications for the business model - consider the new distribution flows, client relationship coverage, broker and partner relationships, reinsurance programme, and how decisions will be taken as to which carrier (UK or EU) will accept risks. Alongside this, build in some flexibility to accommodate subsequent changes as the new market dynamics become clear.
- Target operating model considerations – these include intragroup outsourcing and shared services alongside the governance, risk and compliance model. It's also important to review your human resource model, approach to systems and data (including data protection regulations) and the new controls framework.
- Finance model aspects – considerations include the reporting, capital, balance sheet management and ratings approach, as well as IFRS 17 differences and audit implications.

5

### Programme planning and delivery

- Establish programme governance – as you finalise your Brexit approach, consider the programme team structure and authorities, determine workstreams, develop critical paths and interdependencies, and highlight Brexit scenario contingencies and 'points of no return'. Establish risk logs, budgets and stakeholder engagement, as well as communications plans.
- Workstream activity planning – determine activities and sequencing for workstreams, undertake resource planning, and capture key approval and submission deadlines contemplating readiness activity (such as ability to comply with local solvency reporting, IDD, data protection regulations etc.).



### **Uncertain tax agenda**

Further challenges emanating from an uncertain political agenda include possible tax changes within the US. A move to so-called ‘border adjustment’, under which it would no longer be possible for US insurers to deduct premiums ceded to certain non-US jurisdictions from their tax bills, is still conceivable but increasingly unlikely. Yet legislation including provisions similar to those included in the Neal Bill, which could have much the same effect, is still in train. Insurance costs could rise significantly if such proposals are enacted, which would affect both the availability and price of insurance for consumers in the US. There is also a risk of reciprocal action in markets outside the US, which could lead to the localisation of the global reinsurance market.

Moreover, the international tax system is changing rapidly. A key development is the OECD’s 15 point Action Plan on Base Erosion and Profit Shifting (BEPS). BEPS Action 13 reports, more commonly referred to as Country-by-Country (CbC) reports, will begin to be filed by multinational enterprises before the end of 2017. These reports will provide tax authorities across the globe with unprecedented access to information on where and how (re)insurers do business. While it remains unclear how tax authorities might use such information, the (re)insurance industry can expect increased scrutiny on operations and activities including related party transactions and the potential creation of a permanent establishment outside one’s ‘home country’ (both points in the Action Plan).

Further issues include the US tax authorities’ focus on the difference between ‘insurance risk’ and ‘business risk’ for tax purposes. As the insurance market looks to expand risks underwritten and businesses recognise more and more ‘non-traditional’ risks, it’s important to keep an eye on developments, including ongoing court cases.

### **Navigating political change**

Brexit raises a series of business and operational considerations for UK and EU (re)insurance players to work through.

Alongside this, developments in international tax, the developing business risk environment, and wider challenges to globalisation through increased international political uncertainty add up to global (re)insurers and intermediaries potentially facing greater operating complexities and inefficiencies. Businesses will benefit from keeping abreast of developments and focusing

on identifying strategies aimed at minimising the impact, securing efficiencies as well as opportunities where possible, and developing strong relationships with regulators and wider stakeholders aimed at influencing outcomes. In particular, for global businesses, key will be identifying what needs to operate within nationally regulated borders, and what should be common infrastructure to serve their nationally driven business requirements, to both manage risks and run more cost efficient businesses.

---

## *Make or break*

*The risk concerns at the centre of the boardroom agenda highlight the scale of the upheaval within the industry. While nagging anxieties over interest rates or soft market conditions are still there, the big risks and the big questions that come with them are much more fundamental – what are we in business to do and how do we do it?*

We believe there are four key considerations that your business needs to address in order to turn disruption to your advantage:

- 1 How can you develop the culture of innovation, swift decision making processes and operational agility to respond to fast-changing demands?
- 2 How can you develop the proactive, intelligence-rich underwriting needed to capitalise on cyber insurance and other growth opportunities?
- 3 Are the people you have the people you need to compete in this brave new world? Where can you source the new talent you need?
- 4 Is the structure and business model of your organisation geared to the demands of a more complex global trading landscape?

There is plenty to lose in this new and unfamiliar marketplace. But there is also plenty to play for.

---

## Authors

*If you would like to discuss any of the issues raised in this report in more detail, please get in touch with your usual PwC representative or one of the authors listed below:*


**Stephen O’Hearn**

Global Insurance Leader, PwC  
stephen.ohearn@ch.pwc.com  
+41 446280188

 stephenohearn1

**Arthur Wightman**

Insurance Leader, PwC Bermuda  
arthur.wightman@bm.pwc.com  
+1 (441) 299 7127

 arthurwightman

**Jane Portas**

Regulatory and Insurance Brexit Lead Partner,  
PwC UK  
jane.portas@pwc.com  
+44 (0) 77189 78481

**Paul Delbridge**

Partner, London Market Leader, PwC UK  
paul.p.delbridge@pwc.com  
+44 (0) 20 7212 3085

 paul-delbridge-1b37825

**Domenico del Re**

Director, Actuarial Services, PwC UK  
domenico.del.re@pwc.com  
+44 (0) 20 7213 5720

 domenico-del-re-166b131

At PwC, our purpose is to build trust in society and solve important problems. We’re a network of firms in 157 countries with more than 223,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at [www.pwc.com](http://www.pwc.com).

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PwC does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

[pwc.com/insurance](http://pwc.com/insurance)

© 2017 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see [www.pwc.com/structure](http://www.pwc.com/structure) for further details