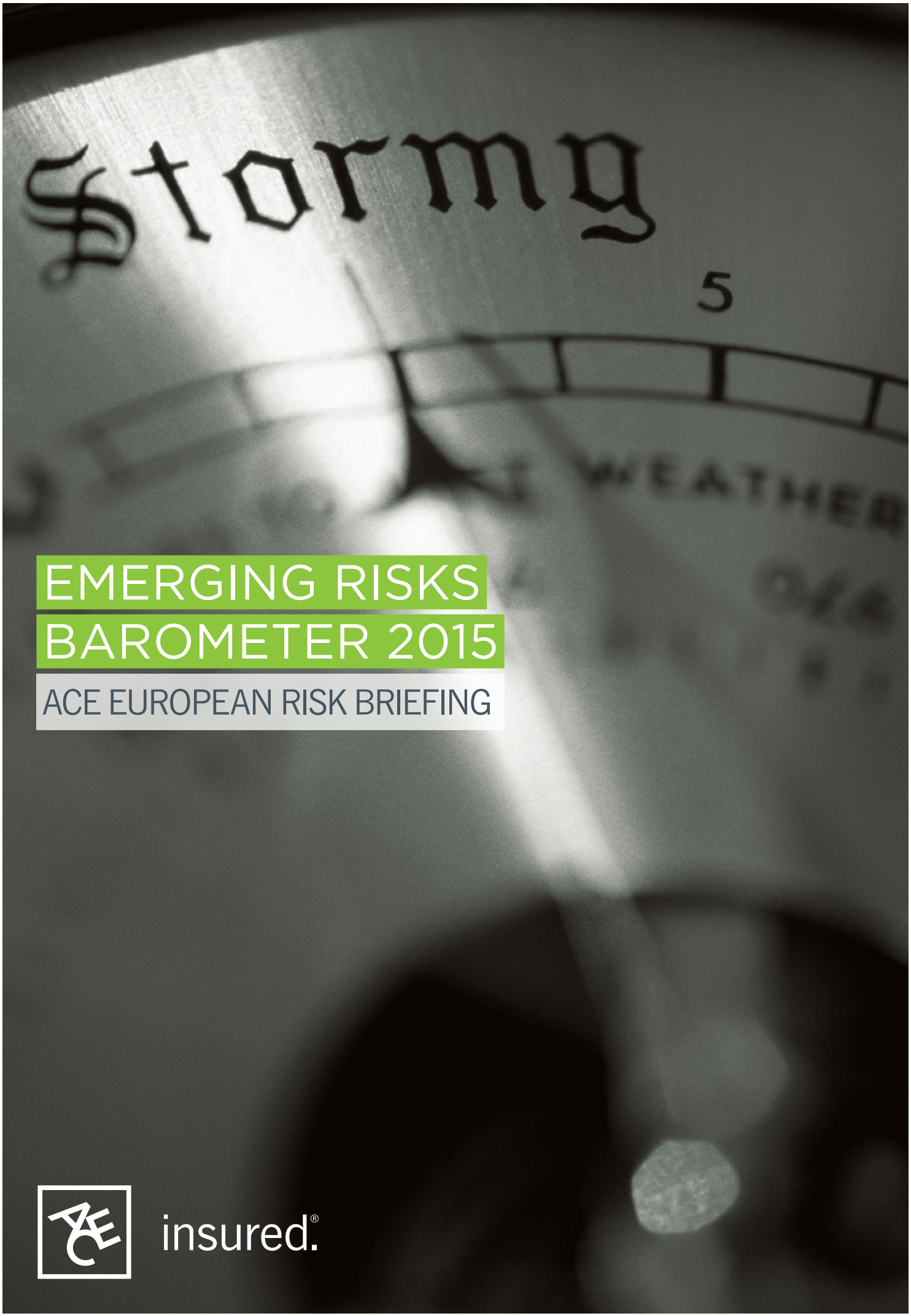


EMERGING RISKS BAROMETER 2015

ACE EUROPEAN RISK BRIEFING

insured®

FOREWORD

BALANCING GROWTH WITH A NEW WAVE OF RISKS

In the two years since we published our first Emerging Risks Barometer, the world has changed dramatically. The global economy has continued its recovery. Businesses across Europe, the Middle East and Africa (EMEA) are pursuing growth and the new opportunities created by emerging technologies. Many are considering opportunities to expand into new regions.

Despite this, one of the consequences of globalised and technology-enabled growth is a new wave of complex, interrelated and fast-changing risks.

Our report highlights particular concern about technology risk. It is the number one emerging risk and the category that consumes the most time and resources, according to risk managers. Respondents generally believe that this risk will also have the most significant financial impact on their organisations. Yet responding to complex technology issues – many of which are closely interlinked with other risks, including reputational, people and terrorism – can be extremely daunting. Companies have collectively invested billions in technology integrity but still suffer continuity issues and breaches. Indeed, these are arguably becoming more frequent and severe.

Supply chain risk also remains front-of-mind for risk managers, with the complexity of expanding supply networks creating numerous interdependencies and exposures. Traditional natural catastrophe-led interruptions are, however, no longer the greatest concern. Our research highlights a range of new reputational considerations moving to the fore, primarily caused by the unmonitored actions of lower-tier suppliers and partners. It is here that risk managers may need to focus their attention.

We also see regulation and compliance risk high on the agenda, especially as companies move into new and less familiar jurisdictions. The direction of travel among Western regulators and policymakers has become clear, with more intrusive supervision and a trend towards direct action against companies and their executives. Emerging markets also continue to drive forward their own regulatory agendas at different speeds. And governments are presenting an increasingly co-ordinated approach – by way of initiatives such as the OECD base erosion and profit shifting project (BEPS) and tighter G8 transfer pricing rules – to tackle aggressive commercial practices by multinational corporations. In turn, many companies admit that they struggle to keep up with the shifting landscape and may need to develop an enterprise-wide approach to managing regulation and compliance activity.

One of the consequences of globalised and technology-enabled growth is a new wave of complex, interrelated and fast-changing risks.

Piecemeal and siloed responses will not succeed in this environment. Effective action will require board-level commitment, an integrated approach and the development of a clearly understood risk management culture across the organisation. These imperatives are not new, but they are increasingly urgent. Risk managers should consider them afresh, asking whether their organisations have made adequate progress since the financial crisis and what can be done to deliver results.

Many are looking for answers from their external partners. Encouragingly for the insurance industry, this report suggests that risk managers regard insurance as a key part of the solution for their emerging risks. But risk managers suggest that it will only remain so if the industry invests more energy in understanding and developing solutions around non-traditional, non-physical risks. We also see a growing need for support beyond financial compensation. Businesses want access to the expertise, advice and capability that delivers an immediate incident response.

The emerging risk horizon is, by its nature, uncertain. But one thing is clear: risk managers will play a key role in ensuring that their organisations have the resilience and contingency plans needed to grow – and thrive – in an ultra-connected, complex and high-risk world.

Andrew Kendrick
President
ACE European Group

EXECUTIVE SUMMARY

BIG THREE RISKS TO WATCH

1 Technology risk

Technology risk – which includes cyber attack, data loss and business interruption as a result of systems failure – is our top emerging risk. Indeed, technology risk dominates our three principal measures of risk magnitude. Almost half the respondents (43%) say technology risk is among their greatest concerns. They also say that it consumes more time and resources than any other emerging risk, and that they expect it to have the greatest financial impact on their business.

Technology plays a role in almost every business's strategic planning – whether in the development of new services or products or as an enabler of operational effectiveness. When it comes to technology risk management, however, our research suggests that companies may not be focusing on the right areas, due to a lack of knowledge about the most likely sources of threat.

Chart 1: Which of the following risk categories are currently causing you greatest concern as a business?

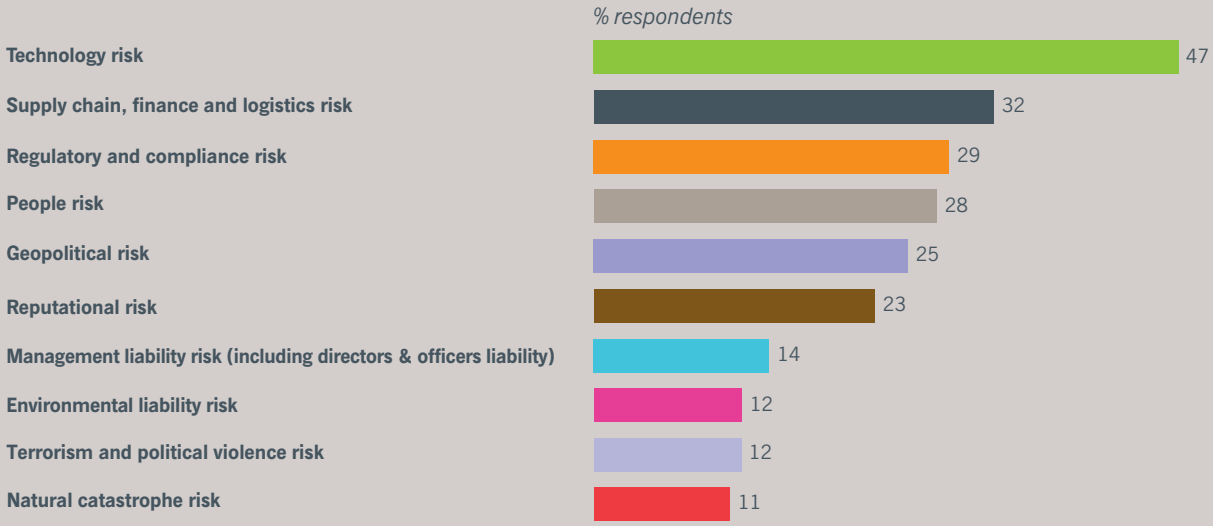
2 Supply chain risk

As in our 2013 Barometer, supply chain risk remains a major concern. As companies expand into new markets – using ever more complex networks of suppliers and partners – the supply chain is at once an enabler of growth and a key source of risk.

In recent years, we have seen major disruptions to supply chains, caused by events such as Hurricane Sandy – which prompted the most extreme fuel shortages since the 1970s[1] – and 2014's widespread flooding in India and Pakistan, which caused US$12 billion in losses[2]. After responding admirably to these and other catastrophes, risk managers say they have achieved a better handle on business interruption risk.

Today, businesses are better prepared and therefore less concerned about interruption caused by natural disasters. Instead, they are focusing more on issues that can harm their corporate reputations. Our respondents rank unethical labour practices as their biggest supply chain worry. Yet six out of ten (61%) admit they cannot always vouch for the ethical and trading standards of every company in their supply chain.

Chart 2: Which of the following risks currently consume the most time and resources in your organisation?

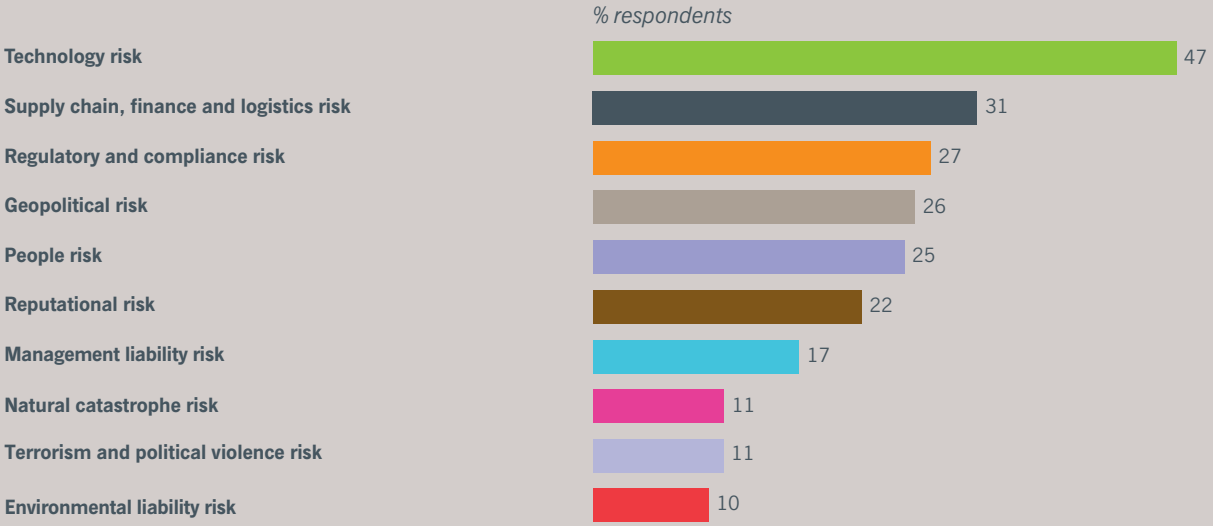


(Don't know / Not applicable: 2%)

3 Regulatory and compliance risk

More than one quarter of respondents (27%) say regulatory and compliance risk is among their greatest concerns. The category also comes third in the list of risks with the potential to cause significant financial impact over the next two years, cited by 27% of respondents, and third in the list of risks consuming the most time and resources (29%).

Chart 3: Which of these risk categories do you expect will have the most significant financial impact on your business in the next two years?



(Don't know / Not applicable: 2%)

While highly regulated sectors such as financial services and energy face the most extreme regulatory challenges, no company is immune. As businesses pursue growth on a global scale, they face a patchwork of regulatory regimes, across markets and jurisdictions.

OTHER RISKS TO WATCH

The rise of people risk

People risk only narrowly missed out on a place in our Big Three Risks. Over a quarter (26%) say this risk – including risks to people, risks caused by people and talent risks – is among their greatest concerns.

One third (34%) say their greatest concern in relation to people risk is time lost to labour disputes. In recent years, we have seen substantial labour action in the UK and Germany as well as in supplier nations such as China. At the same time, three quarters of respondents (75%) say recent global events – such as political unrest in Ukraine and the Middle East – are causing them to review their travel and security policies.

Geopolitical risk to grow in importance?

Regime change, asset confiscation, protectionism and other geopolitical risks also pose a real threat for business. Respondents today are largely confident in their ability to manage this risk, but only 30% say they are very confident. As a quarter (26%) also believe geopolitical risk will have a significant financial impact over the next two years, we could expect the risk to appear higher in the future – especially as companies continue to expand overseas.

Respondents are primarily concerned about foreign governments cancelling operating licences, concessions or contracts. The majority (68%) believe foreign governments are already making it more difficult for them to plan ahead.

THE ROLE OF INSURANCE

Despite considerable debate among risk managers – and even within the insurance industry itself – about the contribution that insurance can make towards managing emerging risks, our survey paints a picture of an industry that is critical in providing corporate solutions. Eight in ten respondents say insurance is an important part of their technology (82%) and supply chain (80%) risk management strategy, for example.

Chart 4: How important is insurance as part of your strategy to manage the following risks?

The insurance industry cannot be complacent, however. Risk managers are looking for more sophisticated solutions to help them manage non-physical risks, which go beyond claims for damage to physical assets. Notably, almost half of respondents (45%) believe the industry could improve its offering around technology risk. Risk managers may believe that better technology solutions could help them 'plug the gap' in their coverage of other top risks, including supply chain and regulatory and compliance risk. As digital technologies are prevalent at all levels of the organisation, risk managers could use tailor-made and wider-ranging products to help protect against a supply chain disruption or data regulation breach that has been caused by technological failure.

Regional variations

There is strong consistency in risk managers' perceptions of risks and their level of concern about these risks.

Technology risk is the greatest concern for all except the UK and South Africa (where regulatory and compliance risk comes top). People risk is the leading concern for risk managers in Germany and Spain.

Risk managers in South Africa and France (in the wake of the Charlie Hebdo attacks) are the least confident in their ability to manage terrorism and political violence risk. Nordic risk managers are least confident in their ability to manage regulatory risk.

German risk managers are least confident in their ability to manage supply chain risk. Supply chain risk is also of greater concern to companies in this market than most other countries studied, perhaps reflecting many German companies' position as exporters.

TECHNOLOGY RISK

Technology risk is the headline story of our 2015 Emerging Risks Barometer.

- Technology risk is most likely to be among risk managers' greatest concerns
- Risk managers expect this risk to have the greatest financial impact on their businesses
- It consumes the most time and resources of any emerging risk
- It is the risk area where insurance is of highest importance
- It is also the area where the market most needs to improve

The growing strategic importance of technology to business, combined with a proliferation of emerging digital-enabled threats, make technology risk a key challenge across sectors.

John Hurrell, CEO of Airmic, warns that the opportunities created by emerging technology in recent years – in areas such as cloud computing and data mining – have been accompanied by new dangers. "How technology can provide competitive advantage is central to companies' strategic thinking," he says. "This has created all sorts of dependencies which, five years ago, simply wouldn't have been there."

Julia Graham, Director of Risk Management and Insurance at law firm DLA Piper, and President of FERMA, says companies must work harder to understand the implications of emerging technologies. "People can be scared of technology risk partly because they don't understand it as well as they'd like to – and people have a tendency to shy away from appearing to be unsure in front of their peers," she says.

Chart 5: Which of the following aspects of technology risk currently cause you the greatest concern?

33%
Hacking/denial-of-service attacks

30%
Systems failure

29%
Advances in digital technology threatening existing business model

27%
Deliberate introduction of malware/viruses

24%
Data theft by third parties

23%
Data theft by staff

23%
Violation of customer privacy/data security breach

19%
Business interruption (e.g. loss of key business applications)

18%
Theft of intellectual property

(Don't know / Not applicable / Other: 6%)

The question that risk managers must answer is whether they are correctly prioritising their various concerns around technology risk. Our study does, however, suggest there are inconsistencies in how they are approaching the many emerging threats.

1. Identifying the true source of the threat
Risk managers' greatest technology-related concern is cyber attack. One third (33%) of respondents say hacking and denial-of-service attacks are their main worry.

This is not surprising. Cyber attackers are increasingly ambitious, aggressive and global. In 2015, UK telecommunications firm TalkTalk admitted to a major breach through which criminals stole personal customer data and used it to steal thousands of pounds[3]. In 2014, hackers broke into Orange France's online customer portal and stole over a million customer records[4].

Risk managers must, however, tread carefully – especially when it comes to identifying where the biggest threats originate. In our survey, for example, almost two in five respondents (37%) dispute the claim that their employees present a greater source of risk than external hackers. They may be mistaken. Verizon's 2015 Data Breach Investigations Report[5] found that internal workers ultimately caused around 90% of data breach incidents – whether through basic error, allowing their devices to become infected, behaving irresponsibly online or losing their equipment.

The emergence of digital disruption as a leading agenda item for risk managers underlines their changing responsibilities.

2. Concern about disruptive new entrants
One important shift in emphasis for many risk managers is that they have begun to think about the threat posed by emerging technologies. Almost three in ten (29%) say the threat of technology advances to their existing business model – 'digital disruption' – is a major concern.

With so many industries facing this risk – high-profile examples include the taxi industry (which has been disrupted by Uber) and hospitality (disrupted by Airbnb) – risk managers' focus on digital disruption is understandable. But this is a new type of threat for which there is no easy solution.

The emergence of digital disruption as a leading agenda item for risk managers underlines their changing responsibilities, with management expecting them to play a more prominent role in the strategic direction of their companies.

3. Establishing a consistent approach
Our survey suggests that risk managers are primarily concerned about denial-of-service attacks and digital disruption, as well as traditional threats such as systems failure. Over a quarter (27%) also cite deliberate introduction of malware as a major threat.

A lower proportion of respondents (23%) say their greatest concern is violation of customer data. While fear of cyber attack will likely include fear of data breach through hacking, it is surprising that the specific threat to customer data is not higher on the list – especially considering that respondents cite loss of customer and sensitive data as the greatest threat to their reputation (cited by 43%). When the personal data of 70 million PlayStation Network users – including log-in credentials, names and addresses – were compromised, Sony estimated its clean-up costs, including the cost of fighting 65 class-action lawsuits brought against the company, came to US$171 million[6].

Emerging technologies posing new dangers

Businesses should strive to improve technology risk awareness across the board, but two emerging technologies stand out:

Cloud computing

Many companies use cloud to store data more cheaply, while start-ups use it to 'scale up' their organisations at relatively low cost. Kyle Bryant, ACE's Cyber Manager for Continental Europe, says that cloud brings risks as well as benefits. "Legal and risk management teams need to be involved in the selection and negotiation stages of the contract to assess the impact on business continuity and insurance," he says.

The internet of things

This collects data from connected industrial networks and enables greater automation and efficiencies throughout the supply chain and production process. Companies are also using data from connected devices, from smartwatches to refrigerators, to create new customer-focused services. But this interconnectedness also creates new cyber risks, to customer data as well as to industrial control systems. According to research by HP[7], 70% of devices connected to the IoT are vulnerable to cyber attack.

The business response

How should businesses respond to technology risk? Some are still in denial, believing the nature of their business prevents them from being vulnerable. "I have heard about medium-sized and big companies that say they don't need cyber coverage," warns Ramon De La Vega, Head of Corporate Risk and Insurance, Telefonica. "It's a really risky assumption."

But progress is being made in the risk function. Among our respondents, 76% say they have increased their influence on digital technology and social media over the past three years.

Businesses that promote an awareness of technology risks throughout the enterprise should become less vulnerable. Encouraging employees to speak out can be important, suggests Julia Graham. "You've got to instil a culture where it's OK to say what you think and report what you see – some clear guidelines, routes of communication and a tone set from the top are all key," she says. "Greater acceptability of the expression 'whistleblower' will also help this situation."

Risk managers need new organisational structures and approaches if they are to combat technology risk effectively:

1. Move beyond silos

Many companies still think of IT as a support function that operates separately from the rest of the business. Yet technology risk is far from an IT issue alone. Julia Graham urges companies to challenge these misconceptions. "Often, the head of information and head of technology work independently – or the voice of the CISO is not heard from within the depths of IT," she says. "Typically, the CISO does not have independent access to the board when perhaps they should. Organisations need to break down barriers to create enterprise-wide risk management."

Cross-functional co-ordination has to involve the IT department, the risk management function and the broader business. That means a new risk governance structure, in which functions share responsibility for technology risk management.

2. Evaluate the business's appetite for risk
Building an enterprise-wide risk culture also means getting to grips with the business's appetite for risk. Some activities require more rigid frameworks than others, while senior executives naturally want to prioritise growth areas.

> Cross-functional co-ordination has to involve the IT department, the risk management function and the broader business.

Risk managers who do not nurture cross-functional relationships cannot hope to capture these priorities, let alone agree practical day-to-day requirements, such as application recovery time objectives or data-loss tolerances. They risk being perceived as barriers to the company's commercial imperatives.

3. Invest in training and skills
The evolving nature of technology risk requires constant investment in the people who combat such dangers. That goes beyond the IT or risk management functions. "Sometimes, good old-fashioned risk management techniques can help," says Julia Graham. "Do a risk assessment, communicate with your people and train your board. Check the compliance of what you do and establish and maintain close liaison on these issues with your external auditors."

Equipping all employees with the skills they need to protect the business from technology risk will pay dividends. Risk-conscious businesses evaluate knowledge gaps, promote skills development and encourage awareness across the enterprise. Risk managers also need to surround themselves with teams equipped to understand the changing nature of technology risk and how to respond accordingly.

4. Stress-test the business
Stress tests and scenario drills help risk managers evaluate their businesses' readiness to withstand technology-related threats. These exercises should be carried out on an enterprise-wide basis, testing the response of every function to, say, a data breach or a widespread systems failure, according to several of our interviewees.

The role of insurance

More than four out of five risk managers in our study regard insurance as essential to managing technology risk. Governments are convinced too. Both the US and the UK governments have undertaken studies exploring the role insurers might play in mitigating cyber risk[8,9]. In the Netherlands, the government's second National Cyber Security Strategy also recognises that insurers can play a major role in insuring residual risks.

However, 45% of our respondents say technology risk is the area where the insurance industry most needs to develop its capabilities. Some say the industry is not suitably mature in its understanding of this category. "They are held back by a lack of understanding, data and experience," says Arie Wouters, Risk & Insurance Manager at NXP[10].

Our study points to several areas where the insurance industry can improve its offering.

Chart 6: In which risk categories does the insurance industry most need to develop its capabilities?

1	Technology risk	45%
2	People risk	28%
3	Supply chain, finance and logistics risk	28%
4	Geopolitical risk	27%
5	Regulatory and compliance risk	22%
6	Reputational risk	19%
7	Natural catastrophe risk	14%
8	Environmental liability risk	14%
9	Management liability risk	14%
10	Terrorism and political violence risk	14%

(Don't know / Not applicable: 3%)

1. Providing broader solutions

For technology insurance to be effective, Edward Smerdon, Managing Partner of Sedgwick's London office, thinks coverage needs to be broader. "Ideally, the insurance needs to cover more than just liability," he says. "It should cover the costs of remedying a breach – hiring a team of IT people to fix the problem, managing relations with customers who have been affected by the data breach. It means managing the PR and the direct financial loss."

Other shortfalls include a lack of coverage for breaches of information held in paper files, exclusions of claims brought by governments or regulators, no coverage of vicarious liability, and no coverage of unencrypted data. Insurers typically price cover on the basis of previous claims histories, but this data may not exist for issues connected to emerging technologies, such as cloud computing and the internet of things.

Covering for reputational damage also remains an issue. "That can really ruin your business," explains Mr Smerdon. "The trouble is no one's thought of a way of compensating a company for loss of reputation. You can't easily prove whether reputation loss was caused by the event in question and put a monetary value on it."

2. Developing more tailored products

One of the issues highlighted in our study is insurers' perceived tendency to package insurance solutions into relatively inflexible off-the-shelf products. Looking ahead, it is clear that risk managers are looking for solutions that are more tailored and flexible. "The industry has to be willing to be educated by its clients so it can develop products to meet their needs," says Kyle Bryant of ACE. "Those insurers that do not deliver a more bespoke service will lose relevance."

3. Improving communication

The insurance industry recognises that it will need to do more to communicate its offering, so that policyholders understand exactly what level of cover they are buying – and what they need to do to ensure their coverage remains valid. "Insurers are doing a lot right when it comes to insuring technology risk," says Kyle Bryant of ACE. "But I don't think the industry has done such a good job communicating to the market."

Looking ahead, it is clear that risk managers are looking for solutions that are more tailored and flexible.

4. Understanding the nature of technology risk

Nick Beecroft, Emerging Risks and Research Manager at Lloyd's, says one of the challenges of technology risk is that it potentially affects the entire business. "Technology risk doesn't respect boundaries," he explains. "But I do think we are seeing the nature of insurance cover evolve quickly to meet those challenges."

If that progress is to continue, insurers will need to invest in new 'tech-savvy' talent – even though there is concern about a shortage of such talent. A recent EY study warned that expertise in new technology is an area where insurers are finding it particularly hard to recruit[11]. Insurers that provide greater focus on recruiting the right people are likely to reap the benefits.

5. New approaches to modelling

New thinking will also be necessary. John Hurrell believes that insurance companies may need to reconsider some of their tried-and-tested approaches to pricing and risk analysis. "The industry cannot rely on the old modelling capabilities and techniques, which basically take historical risk and project it forward," he says. "Insurers need to invest in modelling future risk, based on approaches other than extrapolation of historical data."

> The industry has to be willing to be educated by its clients so it can develop products to meet their needs.

SUPPLY CHAIN RISK

Supply chain risk comes second in the Barometer this year, at some distance behind technology risk.

- Supply chain risk was #1 in the 2013 Barometer
- Today, it is the second greatest concern to companies
- It is second in terms of expected financial impact on the business too
- It is also second in terms of the time and resources it absorbs, but remains well behind technology

A business's supply chain is its backbone: a break has the potential to paralyse much of the enterprise. This is why businesses take supply chain risk so seriously – 31% of respondents placed it among their greatest concerns, more than any other risk category except technology.

Risk managers are playing a bigger role in managing supply chain risk today: 71% say they have increased their influence in this area over the past three years, and 73% say that they have increased their influence over supplier/partner selection. This is encouraging.

The prioritisation of supply chain partly reflects the growing complexities businesses face as they look for growth in new markets. As complexity increases, so will supply chain challenges.

1. Business interruption and natural disasters

First the good news. Since our 2013 Barometer – when the 2011 Japanese tsunami and 2010 Iceland volcano eruption were fresh in the memory – many have improved their response to business interruption from natural disasters.

Almost four in five (78%) say they are confident in their ability to manage supply chain risk (although only 32% are very confident). Arie Wouters of NXP says: "We have a very reasonable understanding of what's out there. We have given supply chain risk a lot of attention in the past few years."

Chart 7: How confident are you in your organisation's ability to manage the following risks?

Progress is to be welcomed – but risk managers cannot afford to be complacent. The five worst incidents in 2014 caused an estimated total revenue impact of more than US$17billion. In one study, four out of five companies said they had experienced at least one supply chain disruption in the prior 12 months[12].

2. Ethical issues come to the fore

Our study suggests natural disasters may no longer be the foremost supply chain challenge. Respondents' most frequently cited concern is that they have unwittingly built supply chains where unethical labour practices are employed – 36% cite this fear.

> Investors and customers increasingly hold companies accountable for practices throughout their supply chain.

Chart 8: Which of the following aspects of supply chain, finance and logistics risk currently cause you the greatest concern?

1	Unethical labour practices in supply chain	36%
2	Non-delivery of, or non-payment for, goods	32%
3	Failure of manufacturing process/quality assurance	23%
4	Transport disruption	23%
5	Product recall	20%
6	Failure to honour buyer or supplier credits	18%
7	Wrongful calling of contractual bonds	18%
8	Piracy	17%
9	Failure of governance (fraud, bribery, corruption)	17%
10	Failure to honour letters of credit or bank guarantees	12%

(Don't know / Not applicable / Other: 8%)

Such anxiety mirrors several recent high-profile controversies, which saw major brands exposed for working with suppliers that did not treat their employees fairly. Daniel Holloway of ACE Group says investors and customers increasingly hold companies accountable for practices throughout their supply chain. One major consumer goods company was criticised last year when it emerged it only required primary suppliers to sign its code of ethics – meanwhile, one secondary supplier was using child labour. When such scandals occur, businesses face long-lasting reputational damage, and it is difficult to restore trust and rebuild lost market share[13].

Insurers also expect greater supply chain visibility. "When we look at large multinational companies, we ask: 'Where is their manufacturing located?'" says Holloway. 'How do they make sure their suppliers are acting ethically and doing what they should?'"

Risk managers have much work to do. More than three in five (61%) concede that they cannot always vouch for the ethical standards of every company in their global supply chain.

Regional differences

Supply chain concerns vary from market to market:

- Unethical labour practices are the main concern for the UK, France, Benelux, Spain and Switzerland
- In Germany, the focus is on product quality (failure of manufacturing process/quality assurance and product recall)
- In Italy, the focus is on contractual obligation (non-delivery or non-payment for goods, wrongful calling of contractual bonds)
- For South Africa, the biggest concern is product recall

3. Complexity mounts

Ethical issues become more challenging as the supply chain grows in complexity. In a major scandal in the UK, when it emerged that major British supermarkets had unwittingly been selling foods containing horsemeat, the company supplying one major grocer turned out to be sourcing its ingredients from 40 different suppliers.

In this climate, every organisation must have a clear top-down view of its supply chain, including the identity and practices of every supplier. As companies are also trying to move quickly and efficiently, dealing with networks of suppliers in multiple markets, this can create conflicts between the need for agility and a thorough, risk-based approach.

The business response

Managing supply chain risk takes up a significant amount of time and resources – 32% of risk managers say it consumes the greatest amount of their time, second only to technology risk. There are steps they can take to mitigate such difficulties.

The risk function needs to develop closer relationships with functions such as procurement that have responsibility for outsourcing.

1. Tighter controls on outsourcing by third parties

Organisations should ensure they have measures in place to control which of their services are outsourced to whom. This can be a considerable challenge. The vast majority of firms in a recent UPS survey said that they did not quantify risk when outsourcing production[14].

The risk function needs to develop closer relationships with functions such as procurement that have responsibility for outsourcing. Agreeing a strategy aligned with the business's ethical values is a good start, while databases such as the Supplier Ethical Data Exchange can help businesses identify partners. Best practice also includes robust and regular audits, unannounced spot checks, and contracts that enable termination for ethical failures.

Athina Pehrman, Risk Manager at Nynas AB, says risk managers must be prepared to rein in the instincts of colleagues with different priorities. "Sales departments and operations people are, generally speaking, most focused on the business side of things," she warns. "Without clear instructions and support from risk management and legal, there is an obvious danger that they might allow or simply miss amendments and don't consider the increased risk exposure that might follow."

2. Simplification and standardisation
Standardised supplier contracts help sales and operations teams become more alert to potential supplier issues. If risk and procurement work together to simplify contracts, ensuring the same level of compliance on ethical questions, it will be obvious when an existing or new supplier is deviating from the norm.

Still, vigilance will be required. "Many companies believe their contract risk is low because they have developed general terms and conditions," explains Ms Pehrman. "But you need to follow up constantly and monitor the use of terms and conditions, templates and adherence to policies; otherwise, there is a risk that unwanted or unquantified exposures or risks are introduced."

3. Reviewing supply chain resilience
Periodic reviews of key areas of the logistics network will identify where resilience can be improved. Enhancements include re-engineering supply chain processes, identifying alternative suppliers, and introducing better contingency and business continuity planning.

Some businesses may baulk at the cost or time involved in such exercises. But research conducted by PwC suggests companies that focus on supply chain resilience, and react to adverse events faster than their competitors, gain market share. The share price performance of such businesses was 7% higher, PwC found[15].

The role of insurance

Global supply chain risk is, by its nature, complex. Without detailed information on suppliers' specific locations and risk details, it is not easily transferable to the market and insurers find it difficult to price.

In some industries, parts of the supply chain can be covered for certain third-party risks. In the main, business interruption and contingent business interruption – largely as an extension of property insurance, due to the unknown nature of the exposures – are used to mitigate risk and protect against financial losses following a disruption.

Despite these difficulties, our study suggests several areas where insurers can improve their offering.

Insurers should develop more integrated policies, working with brokers to bridge traditionally separate business lines.

1. Better packaged solutions
The lack of packaged, holistic supply chain insurance solutions means businesses often buy protection on a piecemeal basis. Not only is this inefficient, but it also leads to gaps in coverage. Contingent business interruption bought as part of a property insurance policy may not pay out in the event of a business interruption where no damage to property occurs.

Insurers should develop more integrated policies, working with brokers to bridge traditionally separate business lines such as property, marine and transportation, casualty and environmental liability. The prize for industry leaders is market leadership around supply chain risk.

2. Additional support on contracts
Insurers can help organisations ensure their contracts with third-party logistics providers and shipping lines provide adequate cover to protect them from physical loss or loss due to delay in getting products to market. Examples include shipping line insolvency, port or channel blockages, political action resulting in closure of canals, or cargo confiscation.

Insurers could also assist in determining risk exposure to clients' stock overseas – in warehouses or in port facilities – from flood, earthquake, political violence or even trade credit.

3. Enhanced reputational risk capabilities
Insurers have yet to address reputational hazard as a major element of supply chain risk, even though previous ACE research suggests businesses feel their reputations are inadequately covered[16].

The support required will take different forms, including provision for financial assistance while firms confront reputational risk incidents and repair the damage caused. Insurers can support with practical crisis management advice. They are also well placed to help businesses head off this risk in the first place, providing assistance to policyholders as they identify and address reputational issues.

4. Assistance with data collection and provision
The data held by insurers gives them valuable insight into where companies are most at risk – whether from a supplier with abusive labour practices or from a particular type of natural disaster. By sharing these insights with policyholders, insurers can help businesses to avert supply chain difficulties and to plan more effectively for the most pressing risks.

At the same time, insurers need to invest in data collection, storage and analytics for their own purposes – most obviously to improve the efficiency of pricing practices.

REGULATORY AND COMPLIANCE RISK

Regulatory and compliance risk is third overall, behind technology and supply chain.

- 27% say regulatory and compliance risk is among their greatest concerns
- 27% say it will have one of the greatest financial impacts in the next two years
- 56% say company directors may not fully understand the governance and compliance requirements in every country for which they have oversight/responsibility
- 68% say that the actions of foreign governments make it increasingly difficult for them to plan for the future

Businesses are struggling with the regulatory burdens they face. This is true for industries traditionally associated with intensive regulation – such as telecoms and energy – as well as for other sectors.

The increasing focus on tax avoidance, for example, has led to an increase in international co-operation between regulators. Companies face new environmental regulation worldwide. And competition and protectionism are providing new challenges.

For multinationals, dealing with this complexity is particularly challenging. But for every kind of business, organisations are struggling with regulatory and compliance risk. Respondents to our survey cite this issue as the third greatest challenge they face (with 27% listing it as a concern).

1. Regulation and compliance in the age of globalisation

Risk managers are concerned about the disruptive effect of compliance: 70% say new regulatory demands are diverting resources from other areas of the business. This may result in missed opportunities. Risk managers may also end up giving other risks insufficient attention.

Almost four in ten (37%) recognise the impact of increased operational costs on their businesses. The same number say it is difficult to keep up with regulatory developments across all their markets.

Chart 9: Which of the following aspects of regulatory and compliance risk currently cause you the greatest concern?

37%	**Increased operational costs following regulatory change**
37%	**Keeping pace with changing regulatory developments across all markets in which we operate**
34%	**Balancing compliance requirements with business demand for growth**
34%	**Implementing major business change in time to meet regulatory deadlines**
31%	**Changes to our industry's competitive landscape following regulatory change**
28%	**Ensuring consistent compliance across our business**
21%	**New requirements around base erosion and profit shifting (BEPS)**

(Don't know / Not applicable / Other: 5%)

John Hurrell of Airmic says globalisation is a critical issue for companies as they manage compliance. "Most of our members are more global than they have ever been," he says. "They are moving into new territories, many of which have unique or unfamiliar risk issues."

2. Regulatory risk as a brake on new investment
Concerns about regulatory risk are a disincentive to making new investments. Sixty-eight per cent of risk managers in our study agree that the actions of foreign governments – which would include the introduction of new legislation – make it increasingly difficult for them to plan for the future.

Yet risk managers are also under pressure to help their organisations manage the risk of new growth opportunities – simply ignoring these opportunities is not an option. More than a third (34%) are concerned about balancing compliance requirements with demand for growth.

For every kind of business, organisations are struggling with regulatory and compliance risk. Respondents to our survey cite this issue as the third greatest challenge they face.

The business response

Companies must become smarter in how they respond to regulation.

1. Common processes and tools
Rather than relying on 'point solutions' to individual regulations, companies would benefit from using best practice from earlier regulatory efforts, agreeing a common set of processes and tools, and adopting a proactive approach to anticipating regulation. An enterprise-wide approach reduces duplication of effort, helping to make the compliance process more efficient and less costly. Some have formed dedicated functions with a brief to work across the organisation, anticipating and responding to regulation and compliance in more streamlined ways.

2. Stronger relationships with regulators
Many regulators have publicly committed to working more closely with businesses – lighter-touch regulation may be the reward for companies with a track record of engagement and compliance that inspires regulatory confidence. Microsoft has worked with European regulators to reach agreements around data privacy and protection in its cloud computing solutions[17].

The role of insurance

Can the insurance industry protect businesses against the changing regulatory and compliance environment?

Certainly, in the case of management liability – which includes directors and officers liability (D&O) – the industry already has an established offering in place. More than three quarters of respondents (77%) say insurance would be important in their handling of management liability over the next three years. Only 14% think insurers should focus on developing their capabilities around this risk.

Beyond D&O, however, businesses believe the industry can deliver multinational insurance solutions that are, at the very least, compliant with regulation in all the territories covered. The industry can also provide additional support beyond financial compensation, such as crisis management, to help risk managers manage regulatory and compliance activity more effectively.

> More than three quarters of respondents (77%) say insurance would be important in their handling of management liability over the next three years.

"The insurance industry is global and it provides valuable help to organisations that are trying to be more global," says John Hurrell. "But it's not helped by the fact that local insurance regulations are so fragmented everywhere."

This theme is at the centre of ACE's 2014 report into the benefits of a multinational insurance programme, which found the top two perceived advantages of such a programme were improved consistency and compliance[18].

In that report, 83% of respondents thought their use of multinational insurance would grow within three years, while 93% expressed concern about the implications of regulatory and compliance change on multinational risk management and insurance. The two findings are often linked: 38% of respondents said environmental liability was an area where multinational insurance might be appropriate; 25% cited political and trade credit risk.

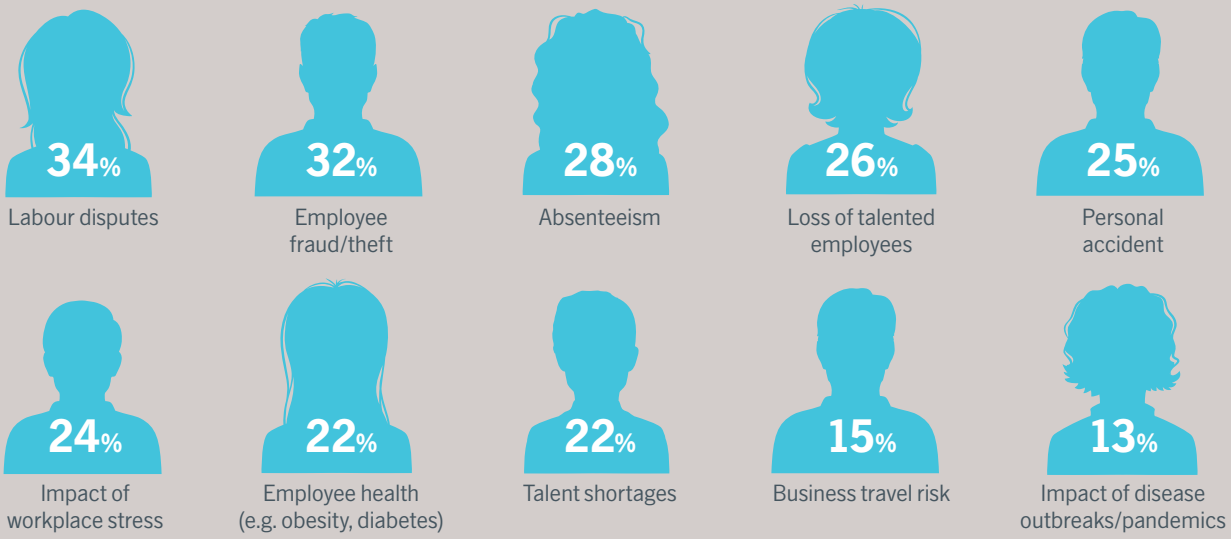
PEOPLE RISK RISING UP THE AGENDA

People risk is respondents' fourth greatest concern in our 2015 Emerging Risk Barometer.

A quarter (26%) of respondents put people risk among their most crucial emerging risks, just one percentage point behind regulatory and compliance risk.

This is a broad category spanning everything from risks related to staff welfare – such as sickness and business travel – to risks connected to staff actions, such as labour disputes and employee fraud. It also includes talent shortages.

Chart 10: Which of the following aspects of people risk currently cause you the greatest concern?



(Don't know / Not applicable: 12%)

1. People risk in the headlines
Recent world events have kept people risk front of mind. Three quarters (75%) of respondents agree that media coverage of terrorist attacks, political unrest and pandemics have prompted them to review their travel and security policies.

2. Labour disputes
Just over a third (34%) of respondents say their greatest concern around people risk is labour disputes. Since our 2013 Barometer, labour disputes have become more common in many countries. In 2014, the Office for National Statistics reported that the number of days lost in the UK through labour disputes in 2013 was up by 79% on the previous year. In Germany in spring 2015, workers had already been on strike for twice as many days as in 2014[19].

3. Risks to employees – inside and outside the workplace
A quarter (24%) of respondents are concerned about the impact of workplace stress on employees. Similar numbers (25%) worry about employees having personal accidents. "We're seeing fewer accidents in the workplace but more outside of work," says Janene Blizzard, Major Risks Underwriting Manager, Accident and Health, ACE Group. "We see a lot of losses involved in commuting. Environmentally-friendly ride-your-bike-to-work schemes have many positive impacts, but they also lead to an increase in accidents. The risk environment is subtly changing."

A quarter (26%) of respondents put people risk among their most crucial emerging risks, just behind regulatory and compliance risk.

The business response

After technology, supply chain, and regulatory and compliance, people risk consumes the most time and resources within organisations (28% of respondents). Our interviewees suggest businesses can manage this risk more effectively.

1. Clarity around ownership
Greater certainty about risk management roles and responsibilities is required for effective people risk management. "People risk often falls in between HR and risk management," says Chris Conyard, Head of Corporate Risks, UK and Ireland, ACE Group. "The business needs greater clarity around responsibility."

2. Renewed focus on industrial relations
With labour disputes on the increase, businesses must improve relations with the workforce and its representatives, including trades unions and works councils. Employee engagement teams, which can be mobilised quickly with the authority to take action when an issue spreads, are one way to manage issues proactively.

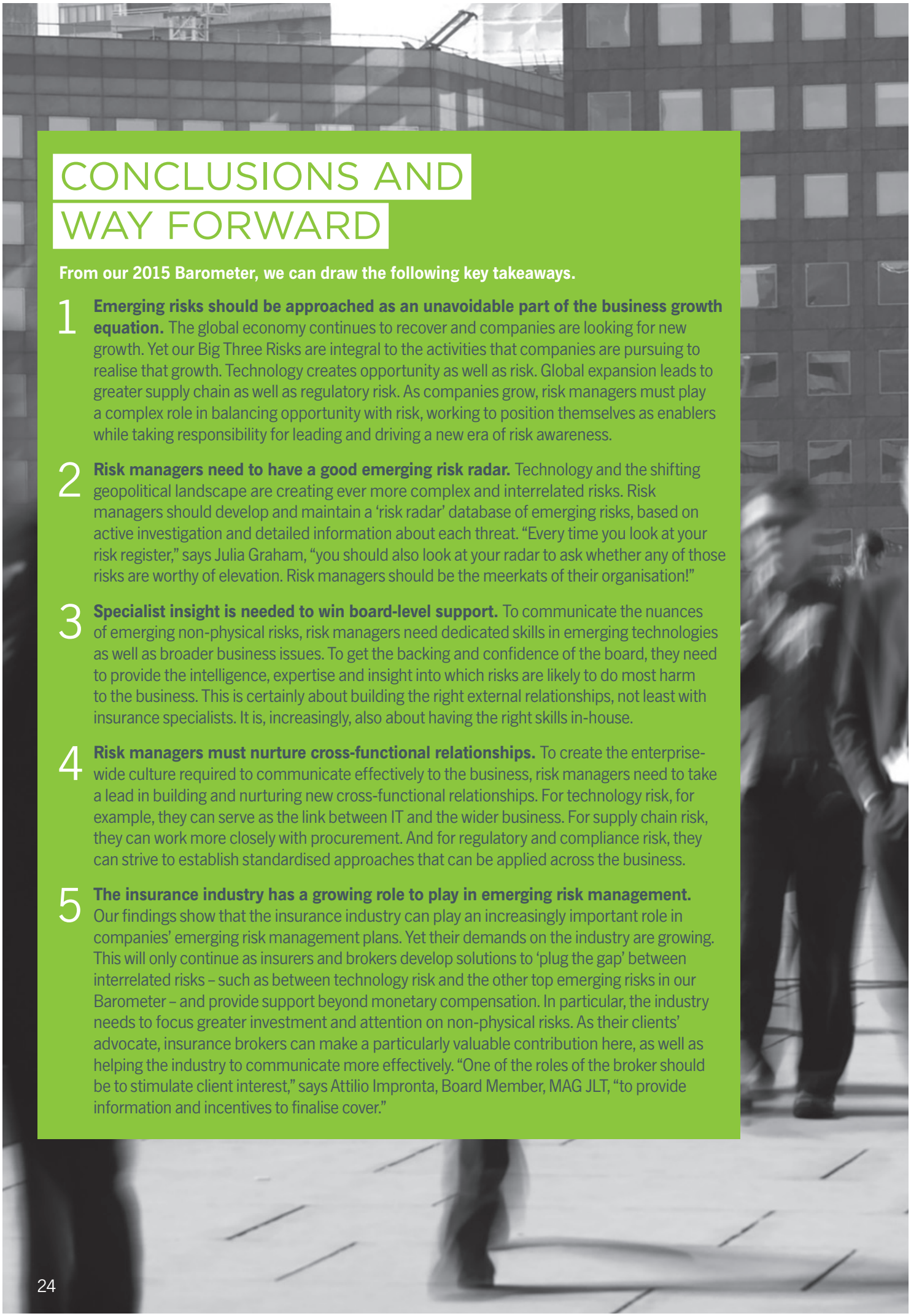
3. Employee benefits and well-being programmes
Employers are introducing flexible benefit programmes, aimed at insuring health and helping staff improve their health and fitness, and reduce stress. Such initiatives may pay for themselves if they deliver greater loyalty, lower rates of absenteeism and higher productivity. Companies may also be expected to ramp up their 'duty of care' activity in line with complex and emerging public health risks, such as diabetes and obesity.

The role of insurance

While 78% of respondents to our study expect insurers to play an important role in their strategies for managing people risk over the next three years, many believe the industry needs to improve its offering. More than a quarter (28%) believe the industry needs better capabilities – only in technology risk was a greater need identified.

In part, there is a need for insurance to offer broader support than financial compensation – including practical advice and assistance. "With business travel insurance, organisations want more than a monetary amount if something happens," according to Janene Blizzard at ACE. "Increasingly, they look for a 24/7 number they can call that will arrange emergency transportation, along with letters of credit for hospitals. Risk managers are also looking for apps to track where their employees are in the world at any time."

But insurers also have an opportunity to develop new types of cover – for example, by helping companies provide attractive offers to their employees. "Employees ask for flexible benefits," says Attilio Impronta, Board Member, MAG JLT, "not just the traditional contract. So companies are seeking wider coverage in this area."



CONCLUSIONS AND WAY FORWARD

From our 2015 Barometer, we can draw the following key takeaways.

1 **Emerging risks should be approached as an unavoidable part of the business growth equation.** The global economy continues to recover and companies are looking for new growth. Yet our Big Three Risks are integral to the activities that companies are pursuing to realise that growth. Technology creates opportunity as well as risk. Global expansion leads to greater supply chain as well as regulatory risk. As companies grow, risk managers must play a complex role in balancing opportunity with risk, working to position themselves as enablers while taking responsibility for leading and driving a new era of risk awareness.

2 **Risk managers need to have a good emerging risk radar.** Technology and the shifting geopolitical landscape are creating ever more complex and interrelated risks. Risk managers should develop and maintain a 'risk radar' database of emerging risks, based on active investigation and detailed information about each threat. "Every time you look at your risk register," says Julia Graham, "you should also look at your radar to ask whether any of those risks are worthy of elevation. Risk managers should be the meerkats of their organisation!"

3 **Specialist insight is needed to win board-level support.** To communicate the nuances of emerging non-physical risks, risk managers need dedicated skills in emerging technologies as well as broader business issues. To get the backing and confidence of the board, they need to provide the intelligence, expertise and insight into which risks are likely to do most harm to the business. This is certainly about building the right external relationships, not least with insurance specialists. It is, increasingly, also about having the right skills in-house.

4 **Risk managers must nurture cross-functional relationships.** To create the enterprise-wide culture required to communicate effectively to the business, risk managers need to take a lead in building and nurturing new cross-functional relationships. For technology risk, for example, they can serve as the link between IT and the wider business. For supply chain risk, they can work more closely with procurement. And for regulatory and compliance risk, they can strive to establish standardised approaches that can be applied across the business.

5 **The insurance industry has a growing role to play in emerging risk management.** Our findings show that the insurance industry can play an increasingly important role in companies' emerging risk management plans. Yet their demands on the industry are growing. This will only continue as insurers and brokers develop solutions to 'plug the gap' between interrelated risks – such as between technology risk and the other top emerging risks in our Barometer – and provide support beyond monetary compensation. In particular, the industry needs to focus greater investment and attention on non-physical risks. As their clients' advocate, insurance brokers can make a particularly valuable contribution here, as well as helping the industry to communicate more effectively. "One of the roles of the broker should be to stimulate client interest," says Attilio Impronta, Board Member, MAG JLT, "to provide information and incentives to finalise cover."

ABOUT THE RESEARCH

This report has been produced by ACE European Group in collaboration with Longitude Research. This is the second ACE Emerging Risk Barometer – the first was published in 2013 – and it is based on two main inputs.

First, we conducted a survey of 500 executives with responsibility for risk management, drawn from 27 industries and 25 countries in the Europe, Middle East and North Africa regions. Surveys were conducted online and via telephone, and respondents were drawn from panels and lists of professionals who have opted in to take part in research.

Respondents represent both larger companies (above US$1bn in annual revenues) and mid-size companies (ranging from US$250m to US$1bn in annual revenues). Longitude Research carried out the survey in early summer 2015, on behalf of ACE. Respondents were chosen at random from a pre-selected database and were screened for eligibility. They were not compensated for their participation and ACE was not identified as the research sponsor.

Second, we conducted qualitative interviews, over the telephone, with a range of senior corporate risk managers and others with expertise in the field of risk management. In particular, we would like to thank the following, who provided in-depth interviews with our research team:

- Nick Beecroft, Emerging Risks and Research Manager, Lloyd's
- Julia Graham, Director of Risk Management and Insurance, DLA Piper; President of FERMA
- Edward Smerdon, Managing Partner, Sedgwick London
- Athina Pehrman, Risk Manager, Nynas AB
- Carlo Casimi, Vice President, Insurance, SAIPEM
- Professor Gordon Clarke, Director of the Smith School of Enterprise and the Environment, Oxford University
- Anthony Fitzsimmons, Chairman, Reputability LLP
- Professor Lawrence A Hamermesh, Ruby R Vale Professor of Corporate and Business Law, Widener University Delaware Law School
- Nicolas Deparday, Director of Corporate Insurance, Michelin
- John Hurrell, CEO, Airmic
- Ramon De La Vega, Head of Corporate Risk and Insurance, Telefonica
- Arie Wouters, Risk & Insurance Manager, NXP
- Attilio Impronta, Board Member, MAG JLT

Endnotes

1 http://www3.weforum.org/docs/WEF_RRN_MO_BuildingResilienceSupplyChains_Report_2013.pdf
2 http://www.theactuary.com/news/2015/04/four-costliest-natural-disasters-cause-nearly-33bn-of-business-losses-and-supply-chain-disruptions/#sthash.FbwCg2Rn.dpuf
3 http://www.theguardian.com/money/2015/feb/27/threat-to-millions-of-talktalk-customers
4 http://www.techradar.com/news/internet/web/more-than-1m-customer-details-stolen-in-orange-data-breach-1247639
5 http://www.verizonenterprise.com/DBIR/2015/
6 http://www.tomsguide.com/us/biggest-data-breaches,news-19083.html
7 http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en
8 https://www.gov.uk/government/publications/uk-cyber-security-the-role-of-insurance
9 http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=df4b3616-0a25-41d1-90dc-ff3734e5d928&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a).
10 https://www.ncsc.nl/english/current-topics/news/new-cyber-security-strategy-strengthens-cooperation-between-government-and-businesses.html
11 http://www.ey.com/Publication/vwLUAssets/EY-insurance-claims-talent-survey/$FILE/EY-Insurance-claims-talent-survey.pdf
12 The Financial Risk Lurking in Your Supply Chain http://ww2.cfo.com/supply-chain/2015/02/financial-risk-lurking-supply-chain/
13 www.airmic.com/sites/default/files/supply_chain_failures_2013_FINAL_web.pdf
14 http://globalsupplychaininstitute.utk.edu/publications/documents/Risk.pdf
15 http://www.pwc.com/us/en/risk-management/supply-chain-resilience.jhtml
16 http://www.acegroup.com/global-assets/documents/Europe-Corporate/Thought-Leadership/ace_reputation_at_risk_july_2013.pdf
17 http://www.out-law.com/en/articles/2014/april/eu-data-protection-regulator-says-microsoft-enterprise-cloud-contracts-are-in-line-with-eu-privacy-requirements/
18 http://www.acegroup.com/uk-en/assets/multinational-research-report-201409.pdf
19 http://www.dw.de/germany-to-mark-record-year-for-strikes/a-18450024

The opinions and positions expressed in this report are the authors' own and not those of any ACE company. This report is for general information purposes only and is not legal advice. We strongly recommend that you review all information with independent tax, legal and finance consultants to assess the structure in the context of your specific situation and cash flows. Any references to insurance policy provisions are not intended to amend or alter any final policy or contract. The terms and conditions of the ultimate, final policy or contract will govern the rights and obligation of the parties.

About ACE Group

ACE Group is a global leader in insurance and reinsurance serving a diverse group of clients. Headed by ACE Limited (NYSE:ACE), a component of the S&P 500 stock index, ACE Group conducts its business on a worldwide basis with operating subsidiaries in 54 countries. Additional information can be found at: www.acegroup.com.

ACE European Group
The ACE Building
100 Leadenhall Street
London
United Kingdom
EC3A 3BP
Tel: +44 (0)20 7173 7000
Fax: +44 (0)20 7173 7800

www.acegroup.com/eu