Global Risk Landscape 2016

BDO

Risk and Opportunity

Nigel Burbidge, Partner / Global Chair - Risk & Advisory Services, BDO

The results of the BDO Global Risk Landscape reflect a changing, more uncertain and increasingly globalised world in which events in one country or market can have a significant impact elsewhere. The aim of the survey is to raise awareness of some of the risks faced by businesses in this dynamic, interconnected and increasingly digitised world and to stimulate debate so that businesses are better prepared and equipped to face the future with more confidence.

Few markets have been immune from the Global Financial Crisis, which continues to impact businesses in many ways today, most obviously through increased regulation and competition. With global regulators stepping up their level of oversight and demonstrating they are willing to cooperate across borders, it is not surprising regulation featured as a key risk across regions.

However, where there is risk there is also opportunity. Updated corporate governance frameworks offer boards the tools with which to improve their risk management, if used correctly. By understanding and recognising risks early, businesses have the opportunity either to manage them to appropriate levels or adapt their business model to turn a risk from something that might damage the business to a positive that might help it move to the next level.

Risks come out of change and nowhere is that more apparent than with technology. The Internet of Things, Big Data and advanced analytics are just some of the new tools offering organisations the ability to offer their customers better and more tailored products and services. But at the same time, there is a risk companies will fail to innovate and fall behind the curve. Cybercrime is another reality of the technology age from which few firms can escape, with more stringent data protection rules being introduced around the world.

The challenge for business leaders is in how they adapt to this riskier world. How they identify and respond to current risks and opportunities and how they identify emerging issues that are likely to impact them further down the line. For large multinationals, adapting their business models is likely to be more of a challenge than it is for their smaller, more nimble, competitors. Whatever the size of business, it will need to develop an approach where the core strategy can be flexed dynamically to take account of external factors.

Resilient organisations - those destined to thrive regardless of the challenge - will have a strong risk radar and the ability to respond quickly and decisively. Conversely, businesses that are slow to adjust to this fast-paced, rapidly-changing world are ultimately doomed to failure.

Contents

A Global View of Risk

The objective of the BDO Global Risk Landscape report was to gauge the perception of risk amongst business leaders around the globe. Not just to form a view of those risks currently high on the radar, but also to assess the emerging risks that will become more of a challenge in the future.

The research, which began in early 2016, gathered qualitative insight from 500 c-suite and senior level experts across 44 different countries, gaining their views on the main risks facing their businesses now and into the future. Organisations varied in size and sector, from mid-sized firms with under 1,000 staff and turnovers of $100m to $500m through to large multi-nationals with turnovers in excess of $10 billion and tens of thousands of employees.

Respondents were asked to rank the risks that have had the biggest impact on their business in the last three years and to anticipate which macro risk trends could have the greatest impact in the next decade. They were also asked to identify those risks which, if managed effectively, could have a positive impact on the business. Important insight has been gathered showing a marked difference in responses between past, present and future risks.

This report offers detailed analysis into the results of this research, offering a snapshot in time into the key concerns faced by business leaders around the world. Accompanied by feature articles it also drills down into a number of risk themes including emerging risk, cyber security and governance.

Dealing with a Riskier World

In a world still to recover fully from the 2008 financial crisis, there remain considerable challenges to doing business. But opportunities abound for the most innovative operators

Eighty-seven per cent of respondents to the BDO Global Risk Landscape believe the world has become a riskier place. Increasing competition, economic slowdown and business interruption are considered the biggest threats overall. Risk mitigation has become the main issue for the largest listed companies while new value creation is seen as the biggest future challenge overall.

In a more global and interconnected world, large corporates undoubtedly feel the full reverberations of commodity price shocks, banking crises, low interest rates, tightening legislation and political instability, whichever market they happen to occur in. Eight years on from the US subprime crisis, the ramifications are still being felt in many economies and regions, in the actions taken by regulators and in the macroeconomic shift of power.

Meanwhile, for the smallest companies, the strong focus on cost reduction remains as they navigate the slowdown. For those businesses with fewer than 1,000 staff, risk mitigation is on the radar, but so is cost management and value creation. It is the more nimble firms that are able to exploit new niches and evolve and diversify to find opportunity in more challenging economic times.

The major risks

Perhaps unsurprisingly, 60 per cent of financial services respondents say economic slowdown is still their biggest threat. This is followed by regulatory risk, with 53 per cent of financial services firms identifying more burdensome regulations as their second main threat. These results very much reflect the world eight years on from the height of the financial crisis, with new regulatory frameworks and more stringent capital requirements for financial services firms in many markets.

"The world is becoming a more dangerous place and going forward there is less certainty," says Nigel Burbidge, Partner/Global Chair Risk & Advisory Services at BDO. "Of the BRIC countries, only China and India are still growing, but China as a manufacturer of goods and consumer of raw materials is playing a much larger part in the global economy. So you've got big trade shifts occurring.

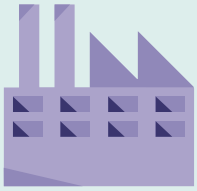
> **THE WORLD IS BECOMING A MORE DANGEROUS PLACE AND GOING FORWARD THERE IS LESS CERTAINTY**

"Traditional manufacturers have been responding by moving their manufacturing to the Far East to get some of the benefit, but China is now increasing wage rates in a compound fashion," he continues. "If you're trying to make decisions going out five to ten years it becomes much more difficult to optimise profitability over a longer timescale. Because technological, environmental and economic change is happening so quickly, people who are looking too many years

FIGURE 1. What are the biggest challenges of the past year by sector?

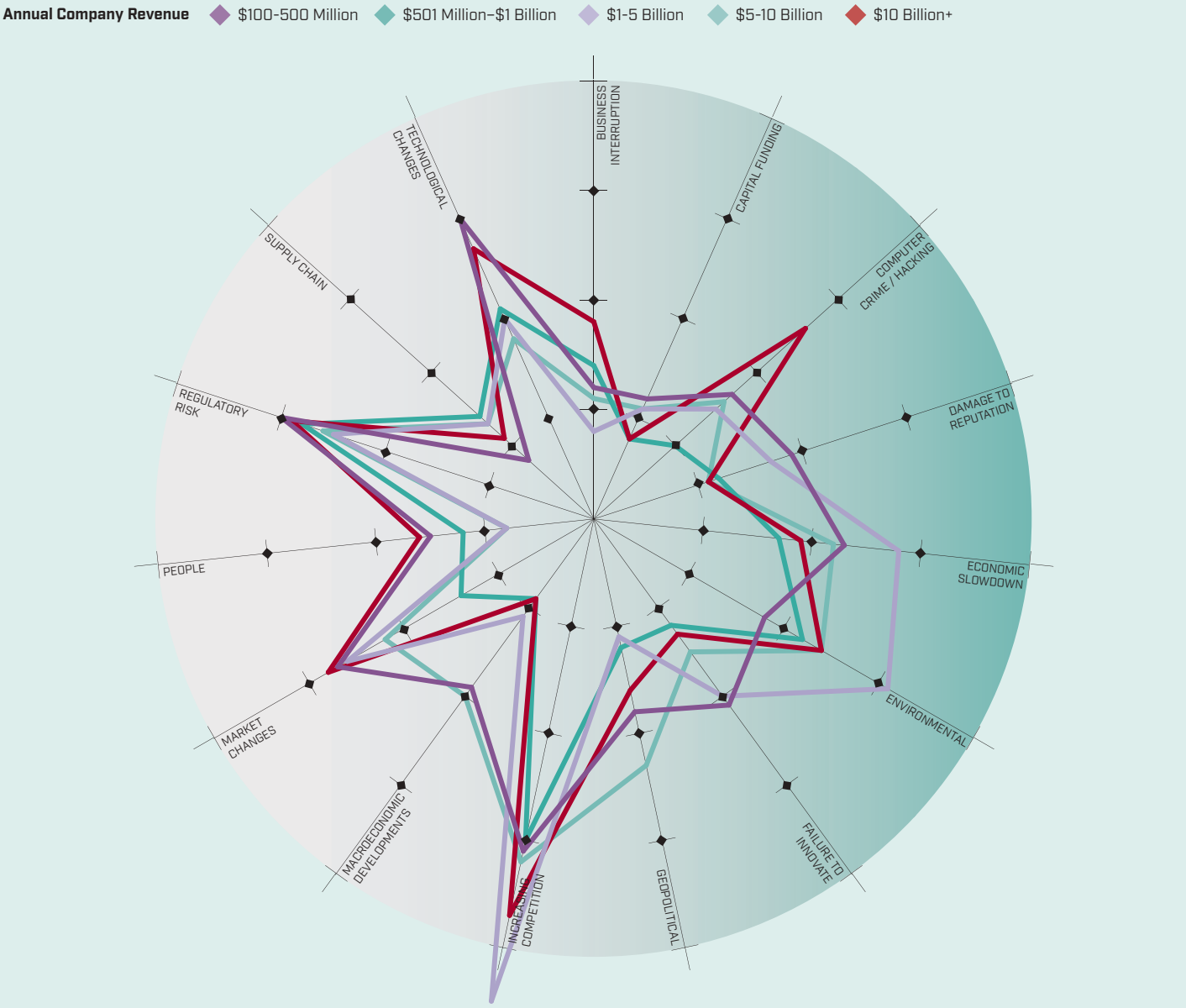
37%
of natural resource companies say **new value creation**

35%
of financial services companies say **risk mitigation**



28%
of manufacturing companies say **cost management**

FIGURE 2. Which of the following macro risk trends do you see as having the most impact in the next 10 years?



ahead stand an increased risk of being caught out.

"If you're a property developer, do you want to be investing in retail parks or do you want to focus on warehouses for the Amazons of this world?" Burbidge asks. "Risk is a double-edged sword. There is the risk of doing the wrong things, but also the risk of not doing anything at all."

Stuttering recovery

With a modest pick-up in global economic activity expected in 2016 (at 3.4 per cent, up from 3.1 per cent in 2015) growth remains subdued, according to the International Monetary Fund's January 2016 update. This is due to a confluence of factors including

THERE IS THE RISK OF DOING THE WRONG THINGS, BUT ALSO THE RISK OF NOT DOING ANYTHING AT ALL

declining growth in emerging and developing economies (for the fifth consecutive year), plummeting oil prices, a slowdown in China and the continuing eurozone fiscal and unemployment uncertainties.

Overall activity is expected to remain resilient in the US, supported by a strengthening construction and labour market. Within Europe, stronger private consumption is expected to outweigh a weakening in net exports, according to the IMF. Forty-three percent of all respondents consider economic slowdown as the main threat to their business. This is highest for respondents in Europe, the Middle East and Africa (EMEA), at 44 per cent, and the Americas, at 45 per cent.

Perhaps unsurprisingly, respondents from EMEA are very concerned about market changes (51 per cent, compared to 44 per cent in Asia-Pacific and 34 per cent in the Americas). With the uncertain future of the European Union and the looming prospect of a Greek or British exit, these issues are clearly weighing on the minds of EMEA respondents. However, 56 per cent think that this risk – if properly managed – could help increase the value of, and results for, their organisation.

"North America and Canada have been a homogenous trading block for a long time, whereas Brussels is still harmonising regulation such that what happens in one European state will also happen in another," says Burbidge. "For a lot of businesses that's probably still seen as being quite an impactful risk."

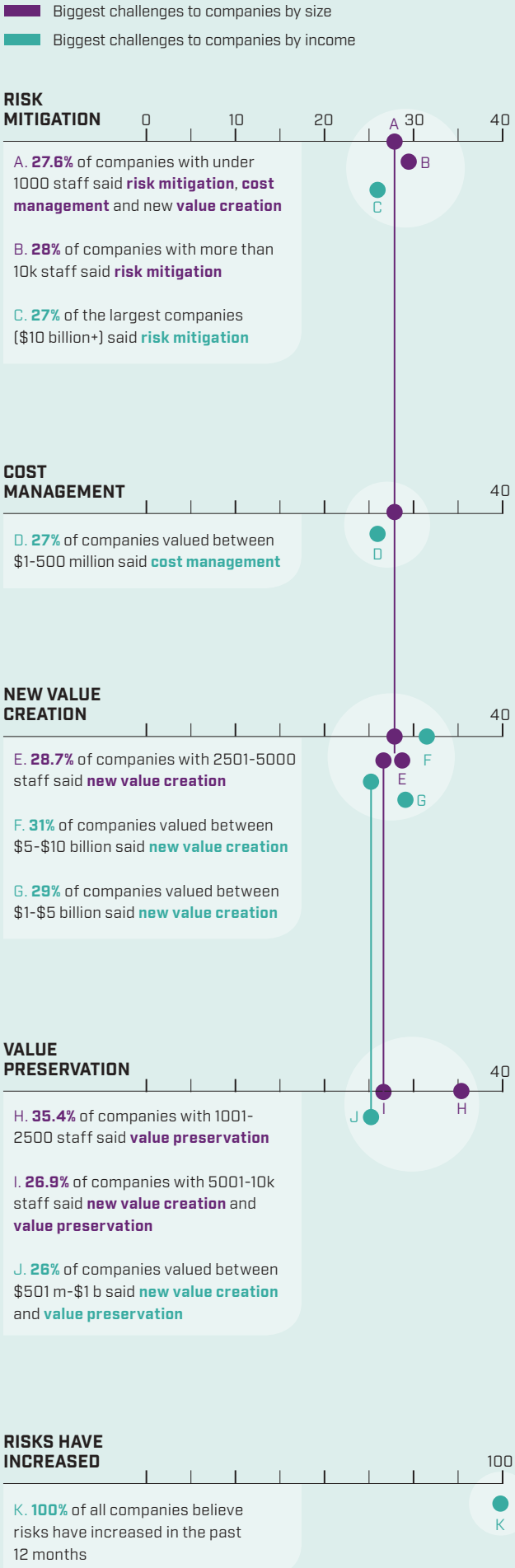
Competitive edge

All three regions are consistent in identifying increasing competition as their current single main threat (56 per cent). Moreover, 62 per cent think this risk would also have the most impact over the next ten years. There are differing views regionally, however, on the need to innovate and meet customer needs to compete effectively. Seventy-five per cent of EMEA respondents, 74 per cent from Asia-Pacific but only 64 per cent from the Americas think the ability to harness technological changes and to innovate and meet customer needs would add significant value.

The relatively lower emphasis from the Americas could reflect the disproportionate number of large business respondents from this region, thinks Julia Graham, technical director at Airmic, the risk managers' association. "Some businesses that need to be innovative are actually very slow-moving and by their nature are quite contemplative.

"Because innovation to some degree requires agility," she adds, "the size of organisations makes innovation with current business models quite difficult."

FIGURE 3. Current Risks



Emerging Risk: The Next Frontier

Tomorrow's major business risks reflect the social and environmental climate far more than they did in the past

The top emerging risks facing businesses in the future reflect major macro-trends including climate change, technological change, resource scarcity and urbanisation. Many of these risks are highly interconnected, as research in the latest global risks report by the World Economic Forum (WEF) demonstrates. This interrelatedness shows how, for example, an environmental risk such as climate change can lead to food and water crises, causing large-scale involuntary migration – all societal risks.

"The risks we have today are increasingly being driven by the context of our world, whereas the risks a few years ago were more likely to be driven by the context of businesses," explains Julia Graham, technical director at Airmic, the risk managers' association. "However, whatever the context, organisations tend towards thinking of risk in the immediate sense and not in the sense of the future – this is what keeps business leaders awake at night.

"Some risks are viewed down the lens in the way they might affect wider society," she continues. "They're typically more complex, connected and their characteristics change with an agility that can be breathtaking, and therefore it becomes much harder to work out how you're going to manage them.

"The organisations which grasp an understanding of risks in whatever context and manage them well are probably also those who will more often turn risks into opportunities," she adds.

Among the emerging risks on the radar of Airmic members, which include a significant number of FTSE 100 and FTSE 250 companies, are terrorism, people and culture, and mass migration.

Terrorism and political risk

The recent terrorist attacks in Brussels, Paris and Ankara and the downing of a Russian Metrojet passenger plane over Egypt indicates that terrorism presents a serious and sustained threat. This is in part due to the rapid rise of the Islamic State (also known as ISIS or ISIL) and risks from long-standing separatist groups. While mass surveillance and counterterrorism have improved substantially in the 15 years since 9/11, smaller-scale attacks still slip through the net.

The mode of attack has also changed. Terrorism experts note a shift in focus from major buildings and assets to "soft targets", with the aim of causing maximum social and economic disruption and fear. While the likelihood of companies being impacted directly is extremely small, the repercussions of such events on business activities are becoming more pronounced.

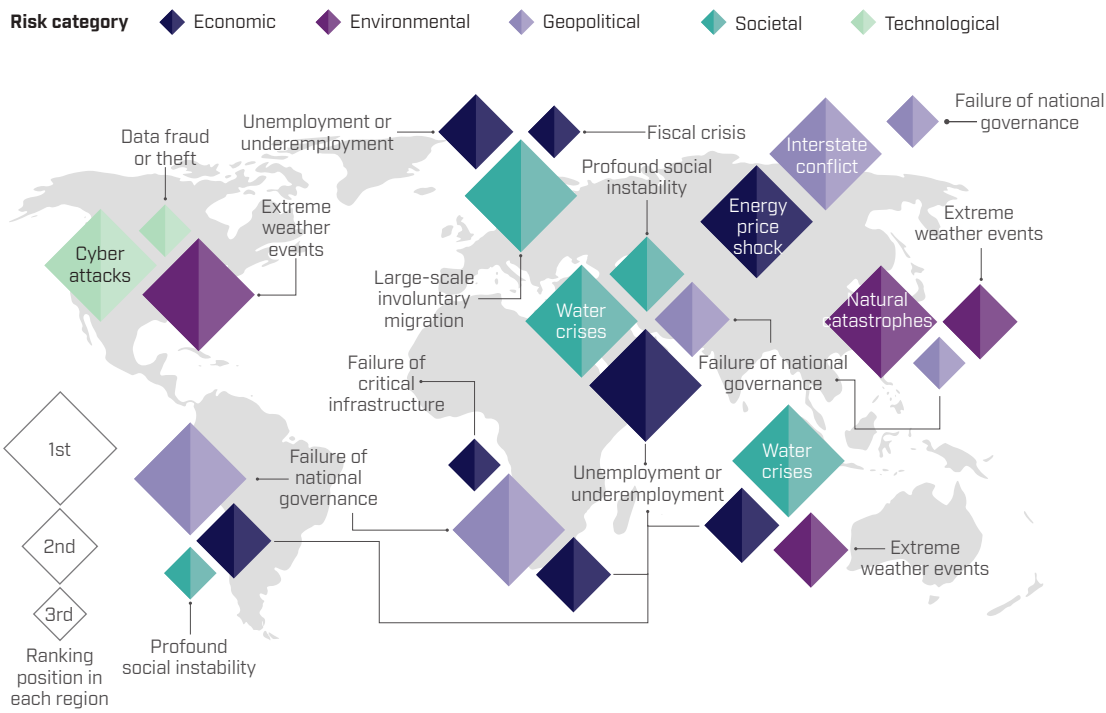
The WEF's Global Terrorism Index shows that the worldwide cost of terrorism in 2014 was $52.9 billion, an increase of approximately $20 billion on 2013 and a tenfold increase on 2000 ($4.93 billion). "I used to go to Brussels every week, when I was chairman of FERMA, the Federation of European Risk Management Associations, and I saw the effects of the bombings in Paris and Brussels first hand," says Graham. "Brussels was understandably in shock and paralysed. This is an enormous issue given the wider impact these attacks have on society and the freedom to mobility and to do business."

Behaviour and cultural risk

According to various studies, the culture on Wall Street encouraged the bad behaviour that was in large part to blame for the financial crisis. People and culture is both a key business risk and enabler, depending on how you look at it, which can significantly boost organisational resilience. Without a positive culture, human error is more likely to be an issue and employees may not feel empowered to question activities that appear suspicious, corrupt or excessively risky.

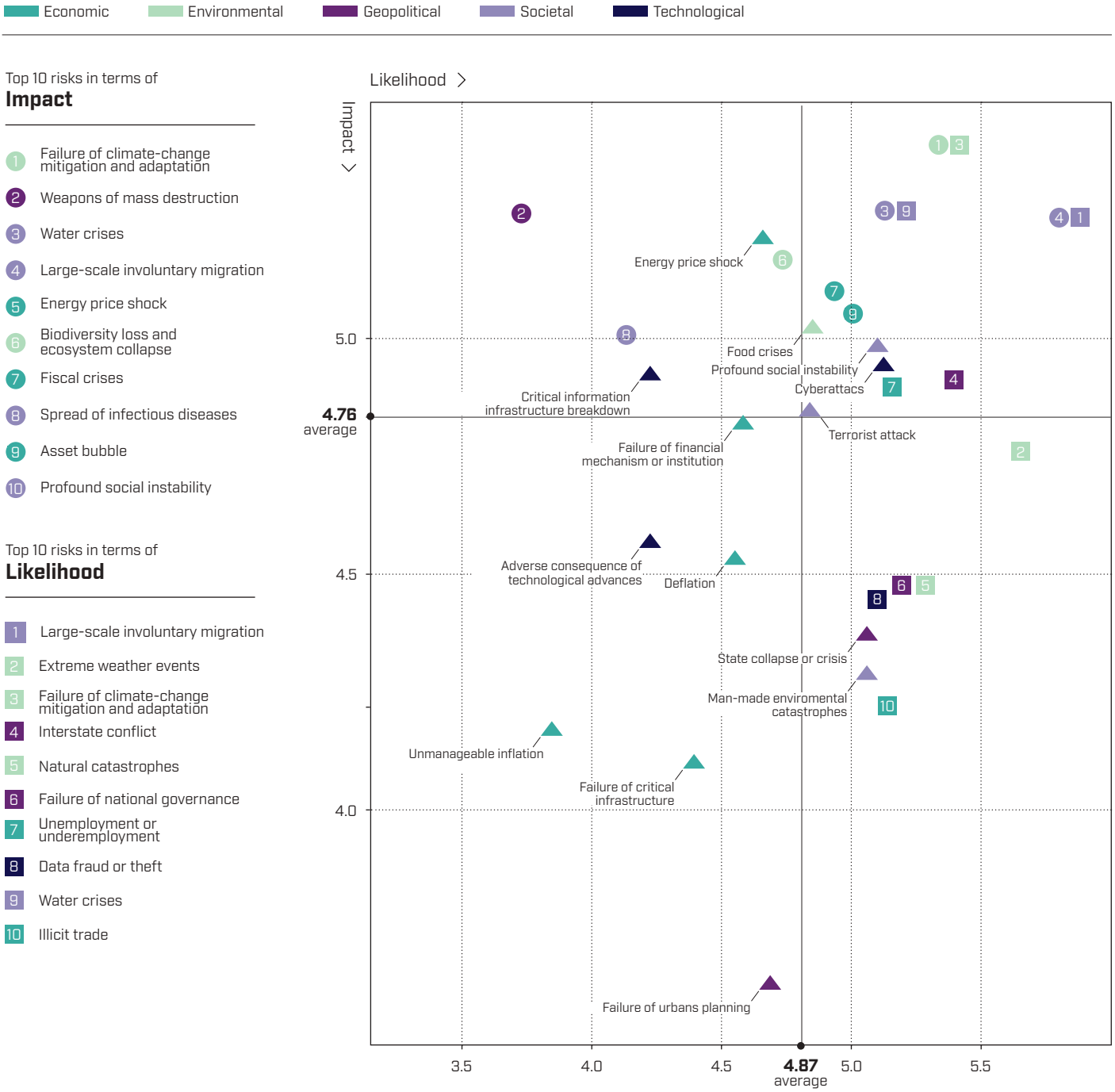
As businesses come to terms with digitalisation and technological change, behaviour and culture will become a critical part of their resistance to cyber risk and their ability to tap new

FIGURE 1. For which global risk is your region least prepared?



Source: *Global Risks 2016 report, World Economic Forum*

FIGURE 2. Key risks: likelihood vs. impact



Source: *Global Risks 2016 report, World Economic Forum*

opportunities. "You can have the best controls in the world but if you don't train people properly to use the knowledge at hand or the support systems at our disposal or to know what to do if something goes wrong, you've got a bigger risk than all the best controls in the world," says Graham. "Most people will tell you that even in the digital world the majority of failures are about behaviour and people, not IT systems.

"People do careless things, people do disgruntled things," she continues. "An awful lot of the issues that arise could be much better managed by training and education and the ability for people to speak out if something looks wrong. If you've got a positive culture where it's okay for employees to tell you if something isn't right without recrimination, that's a great control to have."

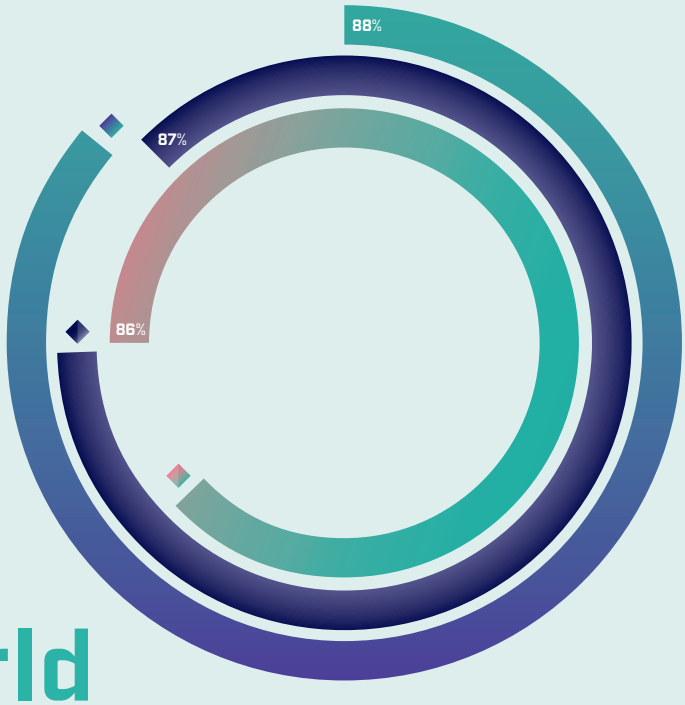
Mass migration

The European migration crisis could just be the tip of the iceberg, according to this year's WEF report, driven by fundamental issues such as climate change and food and water scarcity. Over a million migrants and refugees entered Europe in 2015, with countries struggling to cope with the influx, creating division within the EU over how best to respond.

The risks of humanitarian emergencies, national or regional instability and mass migration will increase, according to the WEF. In the words of a former executive director of the World Food Programme, "without food, people have only three options. They riot, they emigrate or they die." The security implications will be felt by developing and developed countries alike.

But, properly managed, migration presents an opportunity as well as a challenge – both at a country and company level.

FIGURE 1. Respondents who have said risk has increased



IT IS MORE COMMON THAT AN EVENT ON ONE SIDE OF THE WORLD COULD IMPACT AN ORGANISATION ON THE OTHER

A Changing World

The results of the BDO Global Risk Landscape reflect uncertainty in a changing world. Emerging issues such as cyber risk, supply chain interruption and reputational harm increasingly threaten to derail day-to-day business

Forty-two percent of all respondents believe business interruption is currently the biggest threat to their business. While it has always been a significant risk, what is changing is the nature of the perils that can cause that interruption. Traditionally, the main causes might have been fire or natural catastrophe. Today, disruption to business can be brought about by a whole range of events, not all of them related to physical damage.

Business interruption can be caused by pandemic, cyberattack and threat of terrorism (an email threat resulted in the shutdown of over 900 schools in Los Angeles in 2015) – to name just three. From a risk and insurance perspective, as these threats are a result of "non-physical damage", they are not always indemnified under traditional business interruption policies.

The average large business interruption property insurance claim rose to over $2.4 million (£1.6 million) in 2015, according to Allianz Global Corporate & Specialty – 36 per cent higher than the corresponding average direct property damage loss. While most of the top causes of business interruption remain physical in nature, disruption caused by strikes and riots, human error and power interruption – often without evidence of physical damage – were among the top ten.

"If I did a top ten risks assessment ten years ago, they would have been fires and floods and all the physical things," says Julia Graham, technical director at the risk managers' association, Airmic. "Today when you do a risk assessment, they tend to be more about intangible risks.

"Tangible risks are still there, but some ramifications with this change in profile are that organisations have a tendency to focus less on the tangible and turn their eyes towards the intangible – which are more often the risks that can destroy a business," she continues. "This can steal the precious time of the board as these risks are typically more difficult to understand, and to risk-transfer."

Breaks in the chain

In a globalised, highly connected world, business interruption increasingly comes about as a result of disruption within the supply chain. Last year's US labour disputes caused the sudden closure of major ports along the country's West Coast, disrupting imports, including critical components for the automotive industry. Likewise, explosions in the Chinese port of Tianjin affected the global flow of goods for firms within the manufacturing and automotive sectors.

With supply chains becoming more global and practices such as lean manufacturing and just-in-time leaving little room for error, it is more common that an event on one side of the world could impact an organisation on the other. While companies have a high degree of visibility into their first tier of suppliers, things can get increasingly murky further down the supply chain.

Since major disruptive events five years ago such as the Tōhoku earthquake and tsunami and Thai floods, many firms have built more resilience into their supply chains. Nevertheless, with 61 per cent of respondents citing concern over business interruption and supply chain, this exposure clearly remains high on the risk radar. And it is the largest, most global firms that are most concerned about supply chain risk.

Looking ahead, business interruption and supply chain remains a key concern as a macro risk trend over the next ten years. This is particularly the case in the Americas, where 71 per cent identify these risks as likely to have the biggest impact on their business. Supply chain is more on the radar for the larger firms, with 70 per cent of organisations with a turnover in excess of $1 billion saying this risk, if well managed, will increase the value of and results for their business.

Protecting reputations

While damage to brand and reputation remains a relatively

FIGURE 2. Which of the following macro risk trends do you see as having the most impact in the next 10 years?

Risks: **1.** Business Interruption **2.** Capital Funding **3.** Computer Crime/Hacking **4.** Damage to Reputation **5.** Economic Slowdown **6.** Environmental **7.** Failure to Innovate **8.** Geopolitical **9.** Increasing Competition **10.** Macroeconomic Developments **11.** Market Changes **12.** People **13.** Regulatory Risk **14.** Supply Chain **15.** Technological Changes and Development

low concern at present, there is a recognition this will become more of a challenge longer term. In Asia-Pacific 41 per cent of firms expect this will have the greatest impact over the coming decade. This contrasts with just 10 per cent who claim it has been an issue over the past three years.

It could be that reputational risk is seen as more of a concern for the future as brands based in Asia-Pacific grow in international recognition. India and China, for instance, already boast a number of global brands, including Tata, Oberoi and Alibaba. It could also reflect the impact of product recall and ethical scandals, such as the use of child labour, poor working conditions and factory collapses.

Damage to reputation and brand is not just a concern for the very large corporates. A marginally higher proportion of mid-sized respondents (36 per cent of firms with revenue of $501 million to $1 billion) identified this as a present threat versus 29 per cent of respondents from $10 billion-plus multinationals. Mid-sized firms are likely to have fewer resources at their disposal to protect brand and reputation when compared to their larger contemporaries.

The impact of recent data breaches, product recalls and corporate scandals show how quickly such events can lead to a drop in share price and loss of reputation and goodwill.

Under cyberattack

Just under a third of all respondents point to computer crime and hacking as being the main threat to their business, a relatively low number. But interestingly, cyber risk was considered just as big an issue for small to mid-sized firms (with turnover of $100–$500 million) as it was for very large multinationals (with turnover above $10 billion).

Dr. Richard Eiser

The Human Interpretation of Risk

In this article, Dr Richard Eiser, Emeritus Professor of Psychology at the University of Sheffield, looks at the way in which risk is interpreted affects the decisions humans make.

All human decisions involve risk, the chance of something going wrong. So how we interpret risk affects the decisions we make. Some of our decisions are good, some lucky, some unlucky and some plain bad. Bad decisions matter. They cost lives and money, and compromise happiness and relationships. Often this is because risks have been ignored or misinterpreted, but even when we are informed about risks (e.g. by health professionals), our decisions are far from optimal. There are many social, environmental and political barriers to better decision-making, but there are also difficulties arising from the complexity of risk itself and our cognitive capacities for dealing with uncertainty.

Risks are complex

Risk is traditionally defined as the probability of something bad happening. But probabilities can often only be estimated approximately, based on our best understanding of underlying causal processes. This is especially so for rare events and emergent risks, for which there is no adequate previous case history. The dynamics underlying real-life risks can be highly complex, even chaotic, with multiple causes interacting. Consider so-called 'natural disasters'. What turns monsoons, hurricanes, earthquakes and tsunamis into disasters is typically a history of poor human decision-making that acerbates the vulnerability of populations (especially in poorer countries) and critical infrastructure (e.g. Fukushima).

How we interpret statistical probabilities is secondary to how we make choices under uncertainty. Unlike probabilities, choices are discontinuous – to follow or ignore a warning to evacuate, to accept or decline medical treatment, to invest or not invest. Even with accurate estimates of probability, we still need to judge whether any risk is worth taking or too dangerous. The main influences on such judgements include: what others tell us, what we remember, and what we've learnt.

What others tell us

Our readiness to follow advice from others depends, unsurprisingly, on how much we trust them. Trust, in turn, depends largely, but not entirely, on others' perceived knowledge and expertise. Even acknowledged experts may be distrusted if they are seen as biased by some vested interest. Thus scientific and other research needs to be recognised as independent of political and commercial interests. Even non-experts, such as family and friends, may be trusted and imitated more than 'experts' with whom we've no shared interest or personal affinity.

What we remember

Our choices are guided by memory for past events. However, having information stored in our memory doesn't mean we can access it quickly or easily. Memory retrieval is both a selective and constructive process. We look for relevant information on the basis of associations and similarity to the present context. For emergent risks this may mean choosing the best match to previous instances with which we're more familiar, but this remains a subjective process. Rare events (disasters, lottery winnings) attract greater attention (and media coverage) and are more easily retrieved from memory than common events. This leads to a tendency to overestimate the probability of rare events recurring, while underestimating the frequency of common events.

What we've learnt

Learning depends primarily on feedback from the consequences of our actions. Actions that lead to desired outcomes are reinforced and become habitual, those that lead to bad outcomes are avoided. 'Once bitten, twice shy' reflects overcautious avoidance of previously costly choices so that overestimates of risk remain unchallenged by new experience. 'A bird in hand' reflects reliance on immediate over longer-term consequences. Dangerous behaviour may even be reinforced if feedback is sporadic (drink-driving does not always lead to accidents), or so delayed that the costs are disregarded.

Can we do better?

Human interpretations of risk are prone to error, but this doesn't mean we're stupid. Our cognitive capacities have evolved to allow us to make rapid, adaptive and life-saving decisions when faced by extraordinarily complex arrays of information. This requires us ('experts' and non-experts alike) to be selective in the information we consider. This is arguably our default mode of thought. However, we can also, with effort, switch to a slower, more self-critical mode of information-processing, where we test our hypotheses rather than merely seek to confirm them. The first step on this path is to recognise our capacity for error, but also to identify where such errors lie.

Cyber Wars: A 21st Century Disease

As more companies move services online, keeping ahead of cyber criminals will be essential to protect both customer data and corporate reputation

Cyber breaches are now a fact of life for companies of all sizes and from all sectors. As the well-worn FBI quote goes, there are only two types of company: those that have been hacked, and those that will be hacked. This reality has been exacerbated by practices such as bring your own device (BYOD) and the internet of things (IoT), which have introduced weaker links into the chain.

The days of trying to build a fortress are over, explains Steve Rumble, partner and head of technology risk assurance at BDO. "It's a bit like leaving the front door of your house open. You can't assume that your front door is going to be secure now. You're opening up your business model by using technology, and your employees with that, because you're giving them more agile tools to use. So you can reduce your risk exposure but you will never eliminate it.

"If you look at the next five years and recognise that the world is going to continue to change with technology, data and digitalisation and robotics – all these things are going to be at the heart of it – that creates an increasing environment for cybercrime to operate in," he continues. "So organisations have got to shape their governance, education models and people agenda around it. That's why people make these bold statements about cybercrime becoming the disease of the 21st century."

In April 2016, the European Parliament voted for more stringent data protection laws, due to come into force in 2018. The new rules will make it compulsory to disclose if a breach has occurred, within 72 hours where possible, and introduce fines of up to 4 per cent of global turnover for failing to protect sensitive data.

"You've got the cost of recovery, the cost of consequence – whether that's the consumer element, the reputational impact – and it can take a while for that to play out," Rumble explains. "Now you've got the sanctions that can subsequently occur around the new regulations and what that might mean to organisations as well."

High-profile data breaches have demonstrated the significant and often long-term reputational impact such intrusions can have. Affected firms have seen a drop in share price, brand damage, loss of clients and difficulty winning new business.

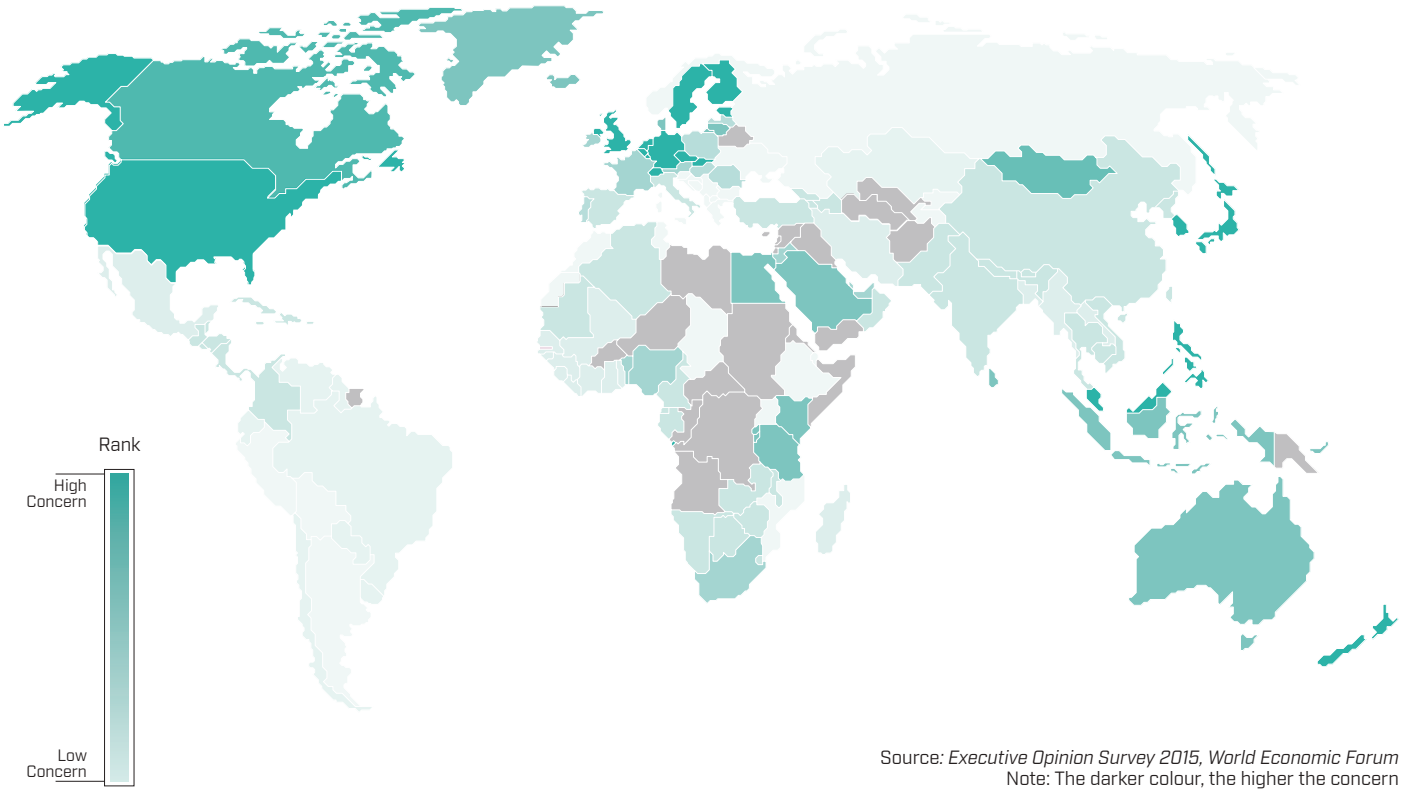
"If there is a security breach and you've lost certain amounts of customer data and you are a consumer brand then that is a significant breach of trust between you and your consumer base," says Stephen Wares, practice leader for cyber risk at insurance broker Marsh.

"As individuals we pass our personal details to consumer organisations and we do expect them to keep those details secure, particularly sensitive details like our financial information or our medical records," he continues. "So for one of those organisations to succumb to a cyber breach, it could be seen as a breach of trust, particularly if it turns out they have not taken sufficient care to secure that data."

48-hour window

With the inevitability of hacks occurring, response plans are also now deemed essential, with the first 48 hours following the

FIGURE 1. Cyberattacks, rank



Source: *Executive Opinion Survey 2015, World Economic Forum*
Note: The darker colour, the higher the concern

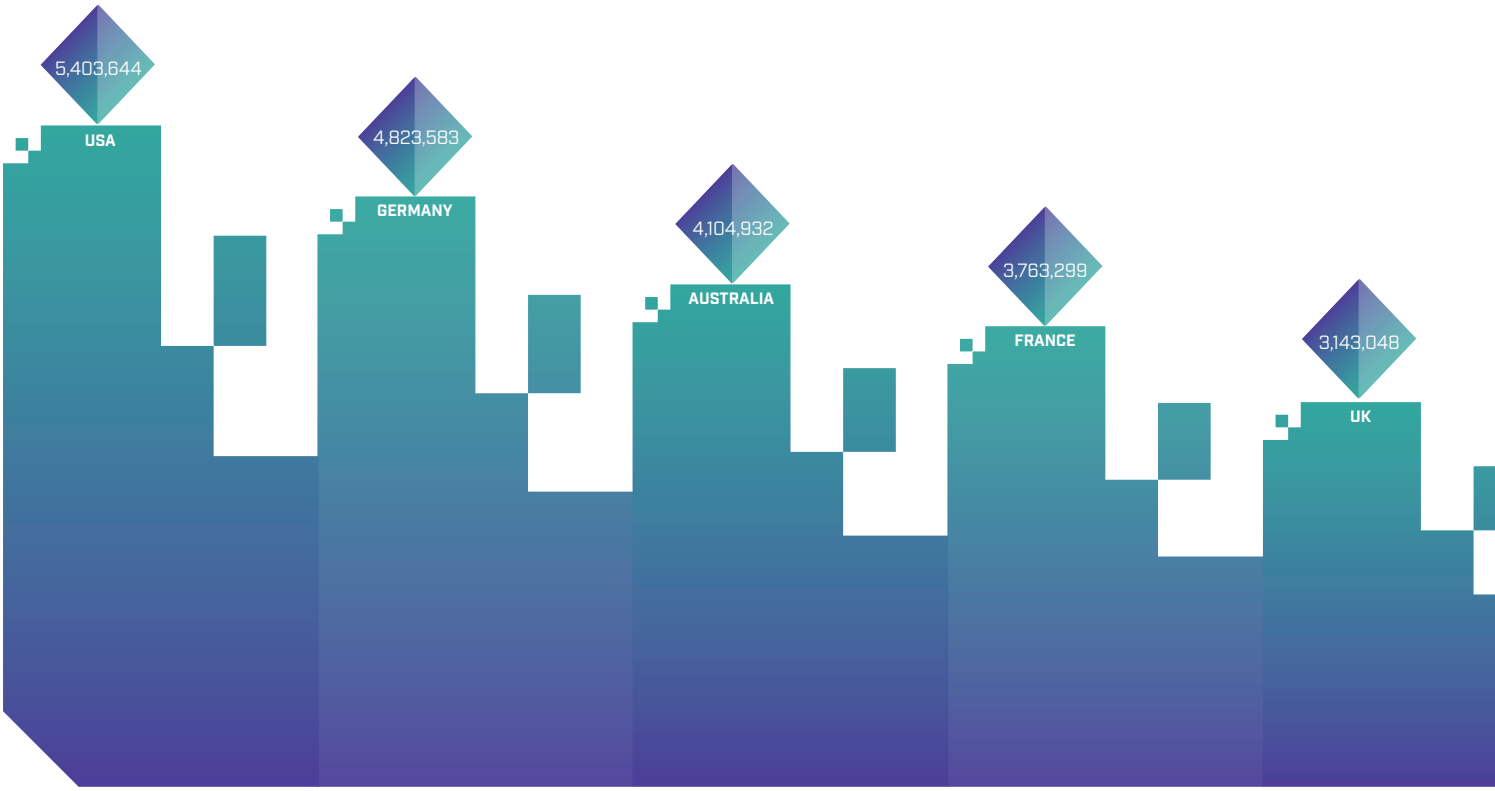
discovery of a hack the most critical time. "If our experience has shown us anything it is that it's important to have a plan," says Jimaan Sane, cyber underwriter at Beazley. "When things go wrong, you need to know what you need to do, who you need to speak to, what vendors you want to bring in and it's important to test and rehearse that plan. Where large organisations are concerned, the way they manage that breach is probably just as important as the breach itself."

Some of the biggest data thefts of recent times were also the most highly publicised and embarrassing. These include Ashley Madison, Anthem, Target, TalkTalk, Sony Pictures, JPMorgan Chase, eBay and Home Depot. In the US, which currently has some of the strictest data breach laws, major hacks have sparked expensive lawsuits, some of them targeting directors and officers.

While small firms may lack the IT security resources of larger firms, data protection regulations do not make special allowances for SMEs. According to one report by the UK Government, 60 per cent of small businesses experienced a cyber breach in 2014 costing on average between £65,000 and £115,000.

This compares to the average global cost of a data breach of $3.79 million, according to Ponemon and IBM's 2015 annual data breach survey. While risk financing is available through the rapidly developing cyber insurance market, products vary. Some policies indemnify first-

FIGURE 2. The average total organisational cost of data breach



Source: *Ponemon Institute / Symantec*

YOU CAN REDUCE YOUR RISK EXPOSURE BUT YOU WILL NEVER ELIMINATE IT

party costs such as business interruption, while others offer third-party coverage for notification expenses and legal costs. Fines and penalties are typically uninsurable.

Globally, there has been a sharp increase in hacking and malware, according to the latest research by Beazley. The cyber insurer found that nearly a third of all incidents in 2015 were caused by hacking or malware, compared to 18 per cent in 2014. Perhaps unsurprisingly, in a year that included the Anthem, Premera and Excellus hacks, the percentage of data breaches in the healthcare sector more than doubled.

Keeping up with the hackers

BDO recommends steps that organisations can take to help protect their data, recognising that attacks often succeed by exploiting misconfigured systems or human error, such as successfully luring employees to respond to phishing emails. So-called spear-phishing exercises use personal information (easily found via social media) to give the false impression of familiarity and entice employees into revealing sensitive information.

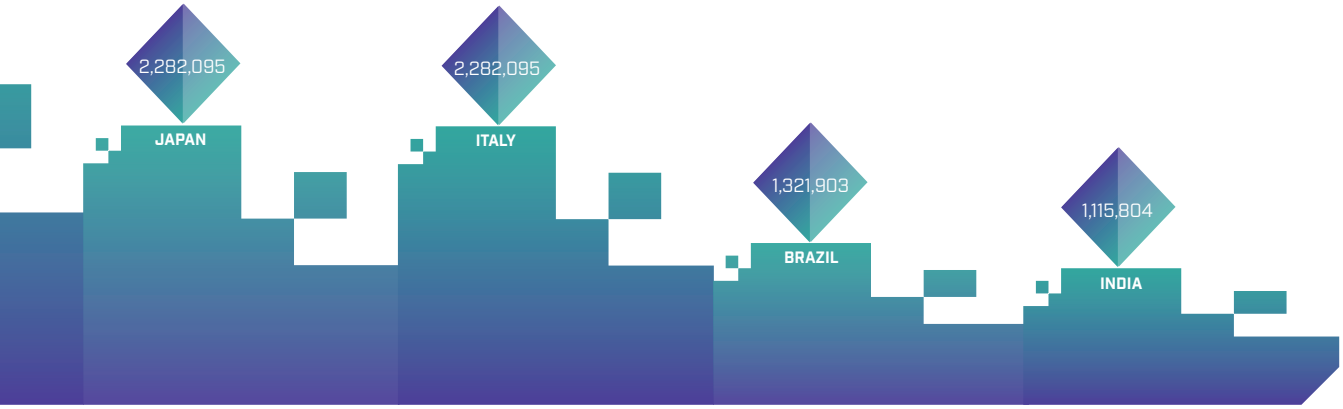
Some cybersecurity firms run simulated phishing campaigns against the employees of an organisation. The aim is to see whether staff will fall for such an attack, unwittingly revealing password and login information. If they fall for it once, there is a much higher chance they will be more alert to genuine phishing attacks in the future.

With 50 per cent of all cyber claims involving an element of human error, it is easy to see why it is important to raise awareness among employees. This is particularly critical as practices such as BYOD become more common in the workplace.

"The level of security for your enterprise network is normally quite high, but it's not always that easy to replicate that same level of security across to an iPhone or an iPad that was designed for consumers and not necessarily with security in mind," says Sane. "It just makes the challenge of security more complicated. It's always a delicate balance between opportunity and security when you are connecting an increasing number of things to the internet."

Larger corporates and financial institutions currently boast the most sophisticated cybersecurity measures, but are also often the most targeted organisations. Among the current deterrents are honeypot computing – where hackers are directed towards a honeypot server, which has nothing on it but is able to detect and contain the intruder – and data loss prevention software.

Measured in US$



BDO's top tips for securing your data:

- **Identify your assets, their location and the risks relating to them: ensure you know what data you hold, where it is stored (and in what format) and the associated sensitivity of that data (eg, personal data, IP, company data)**
- **Obtain threat intelligence information: stay up to date on the threat landscape relevant to the environment**
- **Maintain the security posture by applying a robust patching regime and utilising technical security testing**
- **Create a "culture of security" by championing good cyber hygiene across the organisation: implement a robust training regime that educates employees around the risks to data confidentiality and what their own personal responsibilities are in managing that risk**

The latter can detect where data is stored and replicated. "They are really powerful and can track those datasets and see how they move around," explains Rumble. "So if you start having situations where people start putting attachments into emails it will pick up that this has happened. They're giving you an intelligent view of what's going on in your data world."

While the cost of using the latest security software is prohibitive for many firms, over time this will change, Rumble believes. "Once they've got an established marketplace they'll be able to commoditise it a bit more. All the time you're building tools around this and getting the right brains to think about it. It's all about coming up with new ways of prevention. I'm sure that security experts are currently looking at ways of neutralising ransomware risk."

Environmental Risk on the Horizon

As the world witnesses a steady increase in climate-related natural disasters, environmental risks for businesses are set to become increasingly significant

Environmental risk is a broad term that encompasses climate change, natural catastrophes, sea-level rise and resource scarcity. While environmental issues rank 11th out of 15 possible business threats currently, this rises to third position when respondents are asked which macro risk trend would have most impact over the coming decade.

Many of the survey findings were gathered in the aftermath of the Paris Agreement, following the COP21 meeting in November 2015. Climate change was also hotly discussed at this year's World Economic Forum (WEF) meeting in Davos, with the umbrella theme of "mastering the fourth industrial revolution". And a WEF survey of 750 economists singled out a climate-induced catastrophe as the greatest threat to the world economy in 2016.

It therefore follows that respondents were likely to have environmental risks at the forefront of their consciousness during the survey process. 2015 was also the hottest year on record, with global average surface temperature about one degree Celsius above that of the pre-industrial era, according to the World Meteorological Organization.

"Climate change is exacerbating more risks than ever before in terms of water crises, food shortages, constrained economic growth, weaker societal cohesion and increased security risks," says Cecilia Reyes, chief risk officer of Zurich Insurance Group. "Meanwhile... political conflicts are in turn making the challenge of climate change all the more insurmountable – reducing the potential for political co-operation, as well as diverting resource, innovation and time away from climate change resilience and prevention."

Stormy times ahead

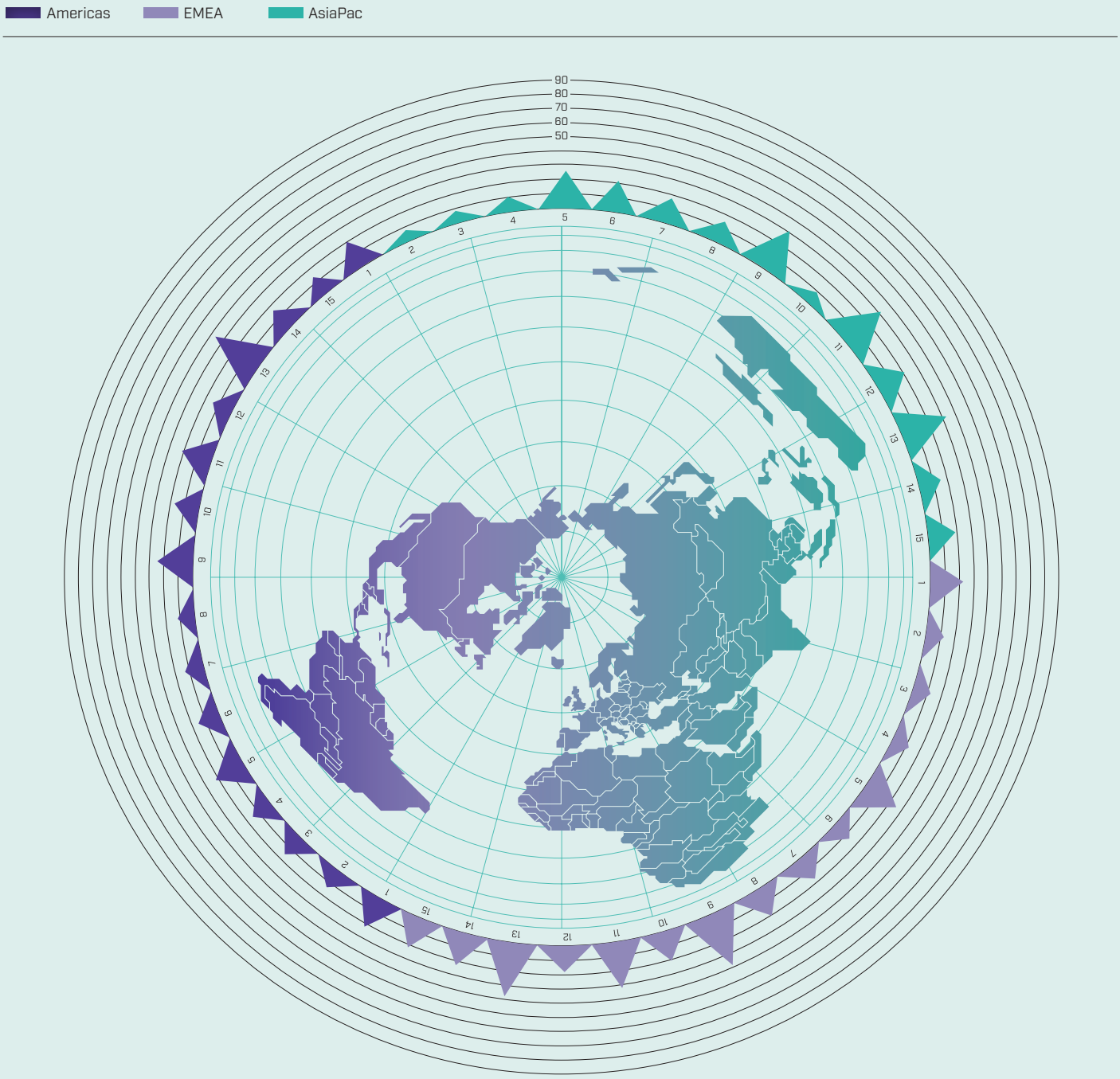
According to the Intergovernmental Panel on Climate Change, businesses and communities should expect to see more weather extremes in the future as a result of climate change. Exactly how this will impact long-term trends is uncertain, but it is clear from the survey results that business leaders from all regions expect environmental risk to become a bigger issue in an increasingly interconnected world.

> **SUCCESSFUL BUSINESSES WILL BE THOSE THAT PREPARE FOR AND ADAPT TO THE CHALLENGES PRESENTED BY CLIMATE CHANGE AND INCREASING RESOURCE SCARCITY**

Currently the biggest concern lies in the Americas. Thirty per cent of respondents across the two continents think environmental risks are the biggest threat to their business, compared to 27 per cent in Asia-Pacific and 25 per cent in Europe, the Middle East and Africa. Looking ahead to the next ten years these figures rise to 35 per cent for the Americas, 31 per cent in Asia-Pacific and 29 per cent in EMEA.

This could be a result of recent costly disasters including severe winter weather in the US in 2014 and 2015, Mexico's Hurricane

FIGURE 1. Which of the following macro risk trends do you see as having had the most impact in the past 3 years?



Risks: **1.** Business Interruption **2.** Capital Funding **3.** Computer Crime/Hacking **4.** Damage to Reputation **5.** Economic Slowdown **6.** Environmental **7.** Failure to Innovate **8.** Geopolitical **9.** Increasing Competition **10.** Macroeconomic Developments **11.** Market Changes **12.** People **13.** Regulatory Risk **14.** Supply Chain **15.** Technological Changes and Development

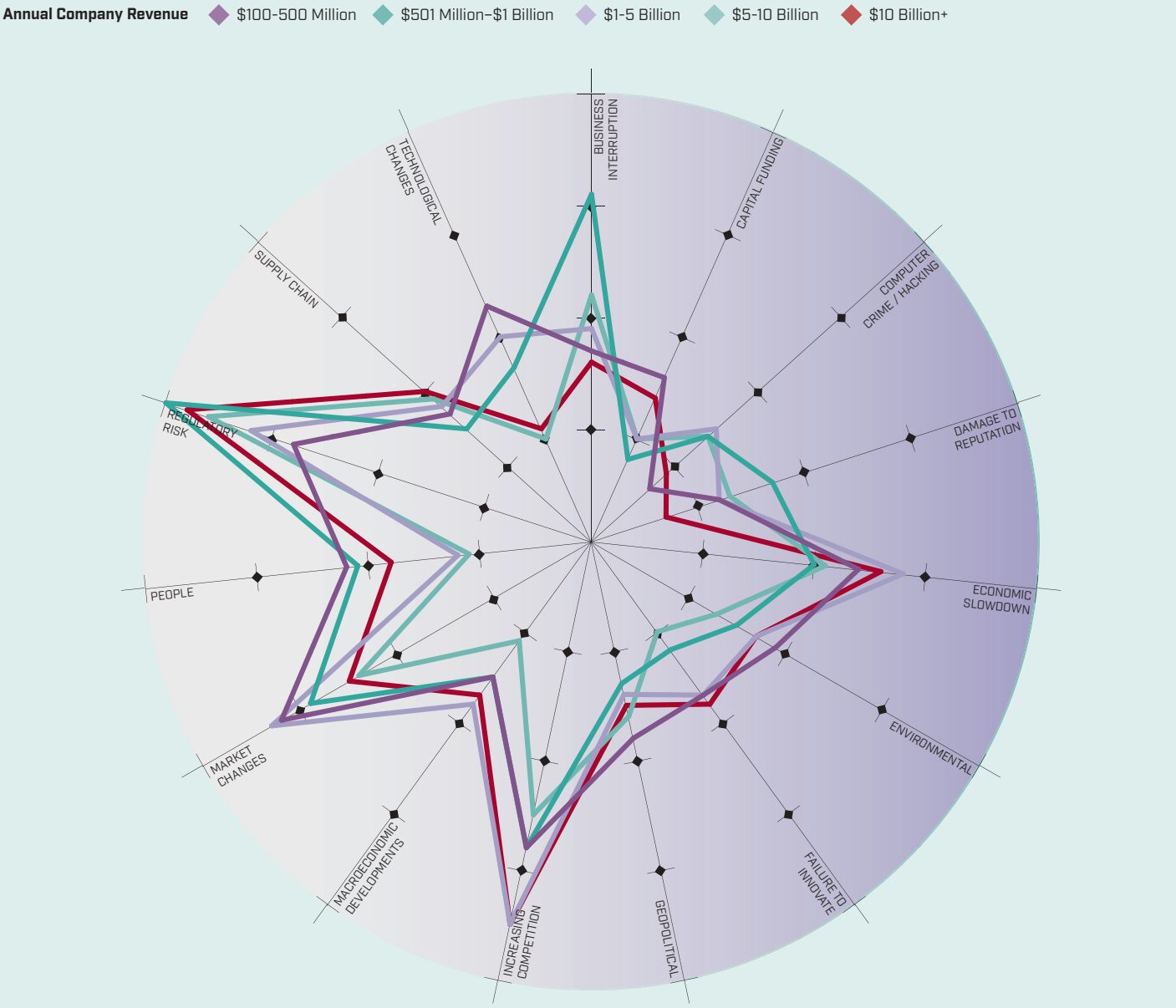
Odile in 2014, the 2013 Alberta floods in Canada, Hurricane Sandy on the eastern seaboard in 2012 and Chile's Maule earthquake in 2010.

As one of the insurance industry's "peak zones" and with its exposures to numerous perils, including hurricanes, earthquakes, tornadoes and floods, the largest catastrophe insurance losses have historically been generated within the US. Hurricanes Katrina, Rita and Wilma in 2005 cost an estimated $60 billion and were only surpassed by the combined losses from natural catastrophes in Asia-Pacific in 2011.

However, it is interesting to note that respondents in Asia-Pacific feel environmental risks have been more prominent to them over the past three years (21 per cent, versus 15 per cent in the Americas and 13 per cent in Europe). Among major catastrophes over the past 36 months are the magnitude 7.8 Nepal earthquake of 2015 and Typhoon Haiyan, which devastated the Filipino city of Tacloban in November 2013. Spurred on by a record El Niño, the 2015 season saw a total of 18 typhoons, with total damages exceeding $10 billion.

The major weather-related events of recent years are clearly being felt by businesses located in

FIGURE 2. Which of the following macro risk trends have been most prominent to you in the past 3 years?



THE MAJOR WEATHER-RELATED EVENTS OF RECENT YEARS ARE CLEARLY BEING FELT BY BUSINESSES LOCATED IN ASIA-PACIFIC

Asia-Pacific. And in an increasingly globalised world, the effects can be wide-reaching. 2016 is the fifth anniversary of the magnitude 9.0 Tōhoku earthquake and tsunami and Thai floods, both major events which disrupted global supply chains in the automotive, manufacturing, electronics and computing sectors among others.

An additional challenge for many catastrophe-exposed countries is urbanisation. By 2025, the developing world will be home to 29 megacities – cities containing at least ten million inhabitants. In such vast, densely populated urban centres, weather-related catastrophes such as typhoons and floods, have the potential to have a much greater economic impact.

Not that Europe has been immune. Winter storms, major floods, earthquakes and hail storms are just some of the natural hazards that have affected parts of Europe in recent years. Particularly costly events included floods and hail storms in Germany and central Europe in 2013. Yet despite their impact, EMEA respondents appeared somewhat less fazed by environmental risk than the other regions.

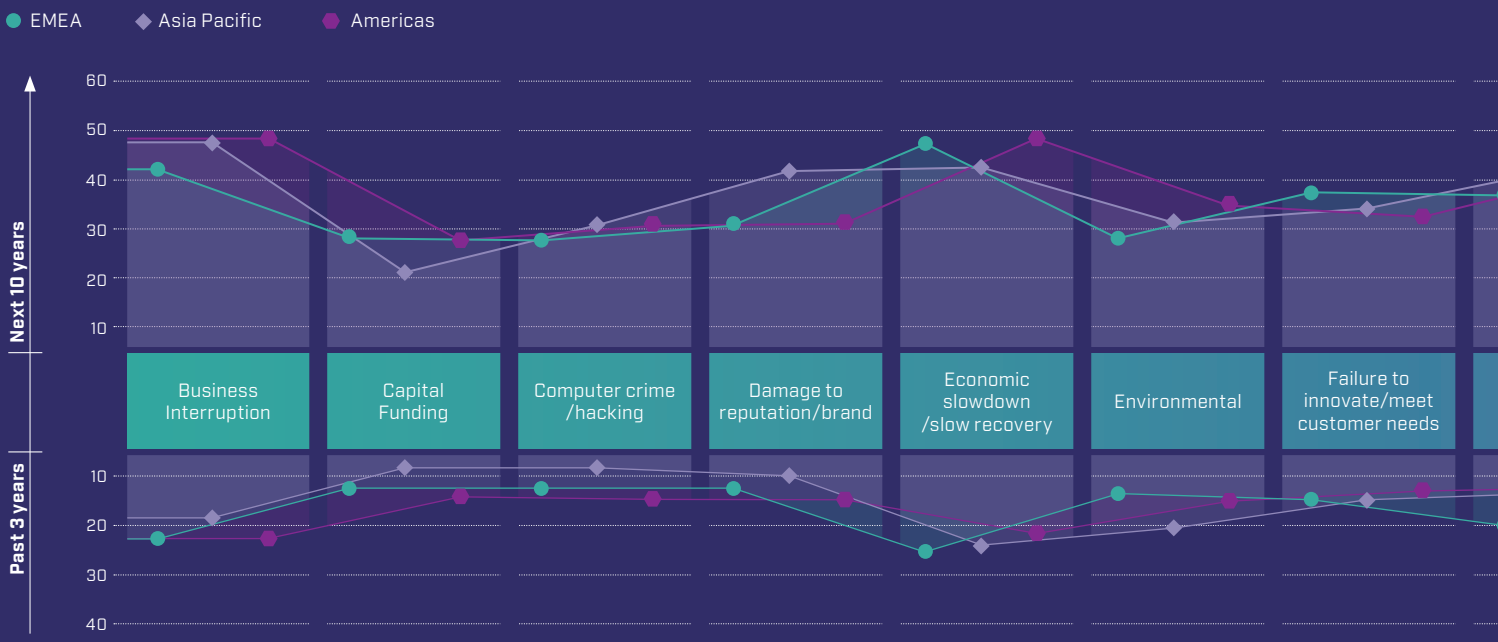
However, for all regions there is a clear concern over environmental risk in the longer term. Successful businesses will be those that prepare for and adapt to the challenges presented by climate change and increasing resource scarcity, by embracing sustainability and developing products and services that cater to cleaner cities, for instance.

"Those companies that ignore climate-related risks are most likely to feel the consequences," state McKinsey consultants Hauke Engel, Per-Anders Enkvist and Kimberly Henderson. "Conversely, those companies that put in place appropriate measures to manage the challenges ahead will not only put themselves in a position to ride out the storm; they could rise above it."

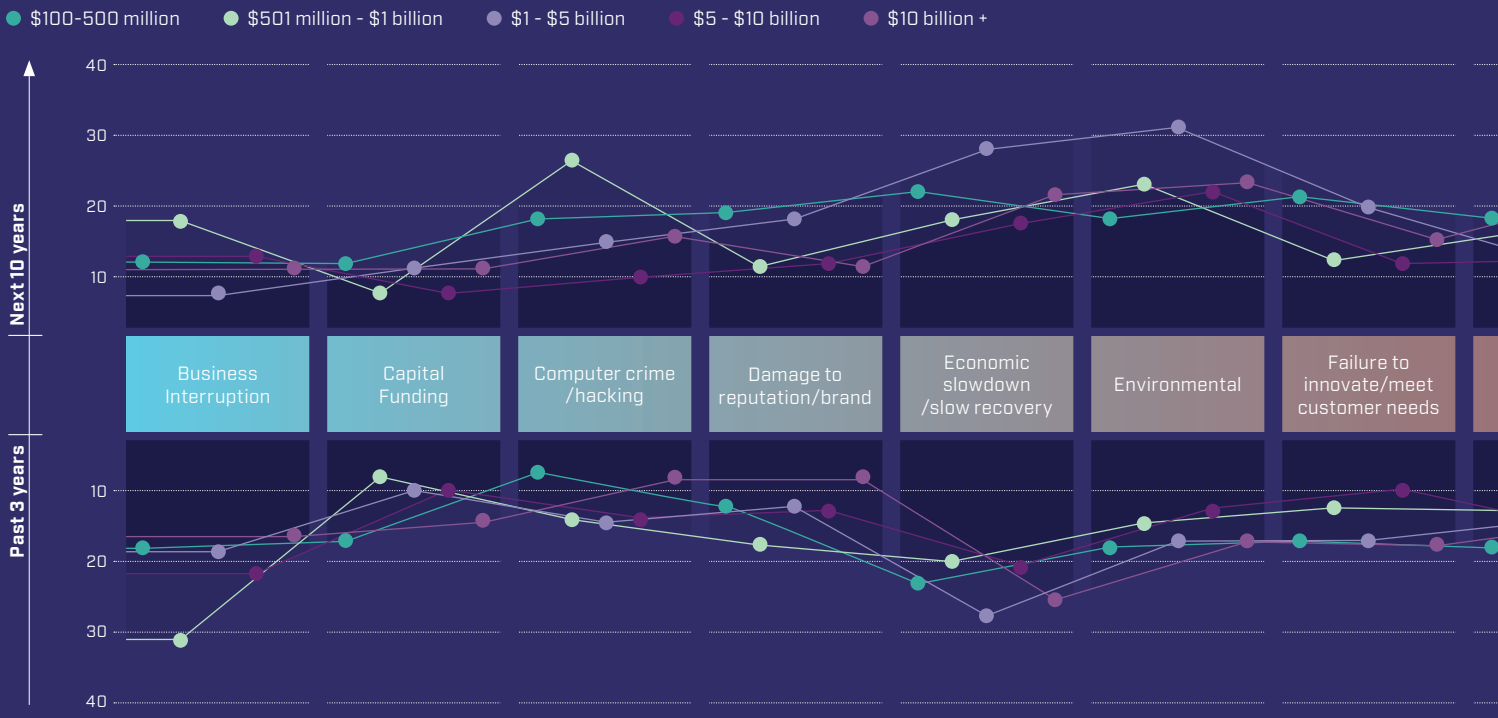
The Evolution of Risk

Looking back, risks have evolved- looking forward risks continue to evolve and differ according to geography and company size

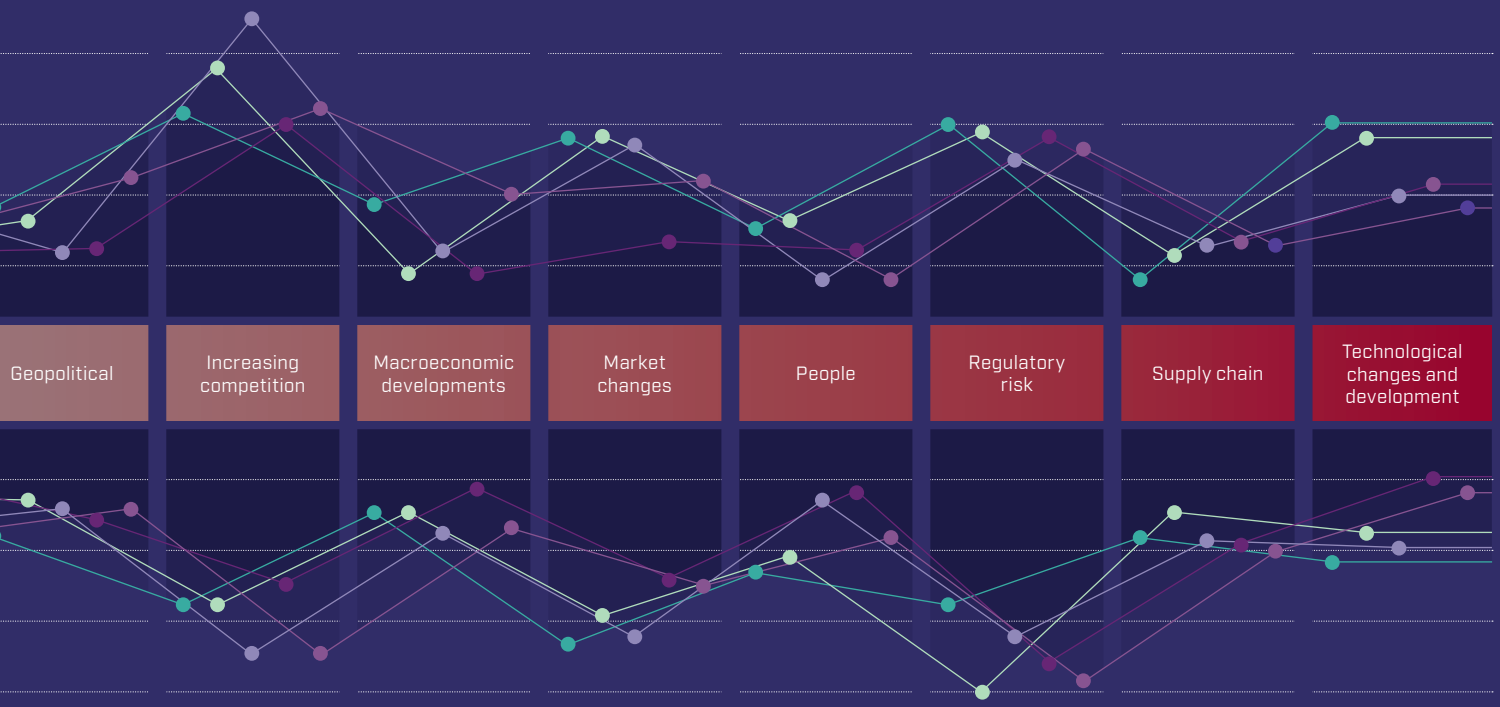
Geographic Location



Company Revenue



FIRMS ARE RESPONDING TO THIS CHALLENGE BY FOCUSING ON BEHAVIOUR AND CULTURE, WHICH COULD INVOLVE FUNDAMENTALLY RETHINKING AND CHALLENGING PREVAILING ATTITUDES TOWARDS RISK



> THE APPROACH BY THE FRC AND COSO IS VERY MUCH TOP DOWN, PUTTING THE EMPHASIS ON BOARDS TO SET THE STANDARD AT THE TOP

Governance: Setting the Tone from the Top

New corporate governance codes have raised the bar on risk management and placed responsibility firmly within the boardroom

It is nearly two years since the UK Financial Reporting Council (FRC) introduced its revised Corporate Governance Code. In the aftermath of the global financial crisis, the revised code intensified the spotlight on effective risk management with an aim of raising the bar for risk management by boards.

An excessive risk-taking culture within financial institutions prior to 2008 has been identified as one of the factors behind the banking crisis, which cost the global economy an estimated $15 trillion, according to the former chief credit officer at Standard & Poor's. Various studies have supported the view that open communication of risk within an organisation is essential to avoiding "board risk blindness".

In its report Roads to Ruin, Airmic, the risk managers' association, identified an invisible glass ceiling that was preventing vital risk information from reaching non-executive directors and other board members. Such a barrier between top management and those that should report to it lies behind many big corporate failures, according to the researchers.

A new era of risk management

The response of global regulators, including the UK's FRC and, in the US, the Committee of Sponsoring Organizations of the Treadway Commission (COSO), has been to bring risk management, appetite and cultures under the microscope. These supervisors now require public companies to share far more detailed information on how risk management ties into their strategy, objectives and governance structure.

Regulators hope this shift in approach will improve the flow of risk information throughout an organisation and embed robust risk frameworks. The approach by the FRC and COSO is very much top down, putting the emphasis on boards to set the standard at the top.

Commenting on the 2014 enhancements, FRC chairman Sir Win Bischoff said in a speech at the Audit Quality Forum event: "The Code recommends that boards be a place of constructive challenge and that 'tone from the top' be observable through the values, attitudes and behaviours displayed right through the company.

"To do so, the board must define the company's purpose, the outcomes it wants to secure, and the behaviours it wishes to promote," he continued. "This involves asking questions and making choices about the correct balance between constructive innovation and disproportionate risk-taking."

As this is the first year of the enhanced reporting on risk and internal controls it is now possible to see how the FRC's changes are bedding in. Early signs suggest listed companies have been slow to adopt the changes, which the FRC puts down to their "substantial and complex nature". Other commentators have put the delays down to the controversial requirement for organisations to include a going concern and viability statement.

"In order to help companies focus on implementing and benefitting from these changes, we will not substantially revise the code for at least the next three years, but rather focus on market-led and collaborative initiatives on succession planning and corporate culture," said Bischoff in a statement.

Speaking the same language

In spite of the delays, Paul Hopkin, technical director of the

Institute of Risk Management thinks the new requirements are a welcome shift in approach. "There are other codes of practice and South Africa is currently transitioning to King IV [the latest iteration of the code of corporate governance issued by the King Committee] and across the world there are several developments. There's a growing obligation on boards to not only understand their business model but to put risks in the context of that business model and strategy.

"The responsibility for risk management is there on the front line," he continues. "And if the board doesn't fully understand the risks and what controls should be in place, they should look for support from risk management professionals, and then from auditors to make sure they've got it right."

South Africa's updated corporate governance code is expected to become effective from mid-2017. While the fundamental philosophy behind King III, which was introduced in 2009, will not change, the updated code will emphasise the importance of risk management to assist companies in considering the interdependencies of risk. In particular, boards will need to consider what constitutes excessive risk-taking, set the level of risk appetite and tolerance and demonstrate they have an appropriate level of oversight throughout their organisations.

Meanwhile, under COSO, boards are being challenged to effectively oversee the organisation's enterprise-wide risk management in a way that balances managing risk while also adding value. It is the old adage that effective risk management is not just about identifying areas of potential vulnerability, but also spotting and exploiting opportunities as they arise.

While a top-down approach is important, Hopkin thinks a strong connection between the board and people at an operational level within an organisation must be maintained. "You need to connect the information that's available from operational people, who understand the business model and today's risks, and you need the opinion and views from people at the top, who make the risk-based decisions going forward.

"It can be quite a challenge," he adds. "Do the two approaches complement and reinforce each other or is there a disconnect?"

One way risk management professionals can avoid a disconnect is by learning to speak the same language as the board. Gone are the days of technical jargon-filled risk registers and in their place a shift in language and approach. But what hasn't changed is the ability to weigh up short-term pressures with longer-term goals and objectives, and to communicate this effectively.

"If you talk to the board about the business model and risks within that business model then you have a much more engaged board," explains Hopkin. "This is because you've got them talking about how the company works, adds value and makes its money... and then you can engage them on the risks."

The FRC's revised Corporate Governance Code requires listed firms to:

- **Confirm that a robust system of risk management has been developed and is fully integrated into normal management and governance processes (eg, business strategy and planning)**
- **Define and articulate their appetite for risk in key areas**
- **Describe their principal risks and how they are being managed**
- **Confirm the identification and assessment (eg, via techniques such as stress and reverse stress testing of all principal risks)**
- **Review and confirm the ongoing effectiveness of key operational, financial and compliance controls**
- **Communicate, incentivise, embed and measure behaviours that create a strong risk and control environment and confirm the existence of an appropriate culture**
- **Consider how much assurance you need over the risk management process, how it will be objectively obtained and what should be communicated externally**

FIGURE 1. Respondents who said rate of change was fast

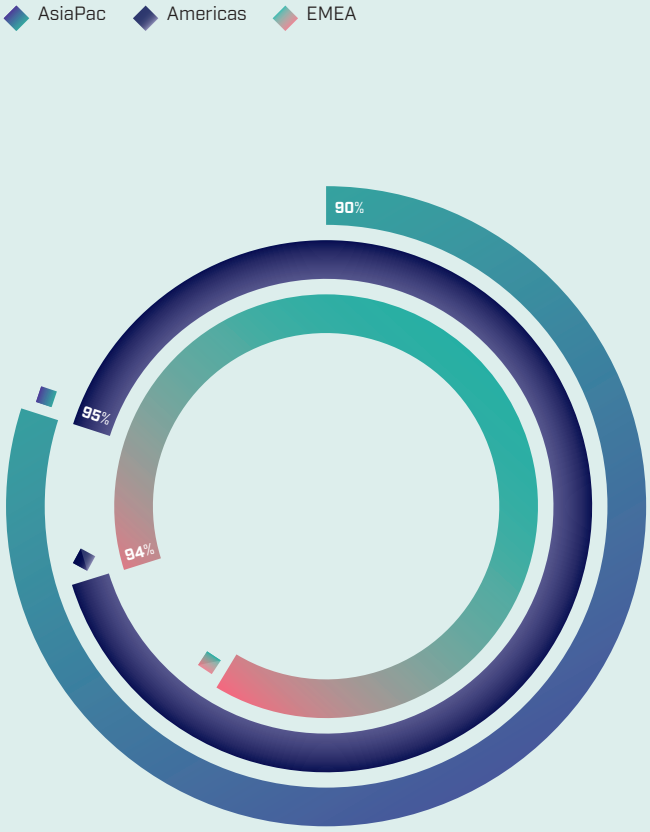
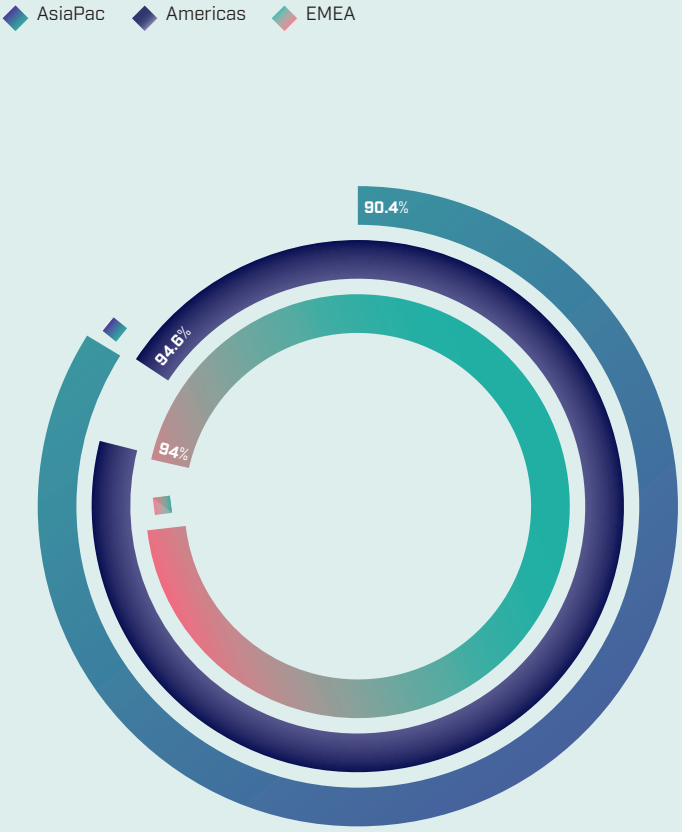


FIGURE 2. Respondents who said risk was increasing



The Long Arm of the Regulator

Regulators worldwide are a tougher breed in our post-financial crisis world, meaning new compliance challenges for businesses

The aftermath of the financial crisis, where supervisors around the world were considered partly responsible for failing to prevent the misdemeanours of the banking sector, has resulted in a tightening of regulatory frameworks. And not just those governing financial services. Across many industries, new and amended laws surrounding bribery and corruption, environmental protection, and health and safety – among other things – mean much greater oversight than in the past, with enhanced powers to take wrongdoers to task.

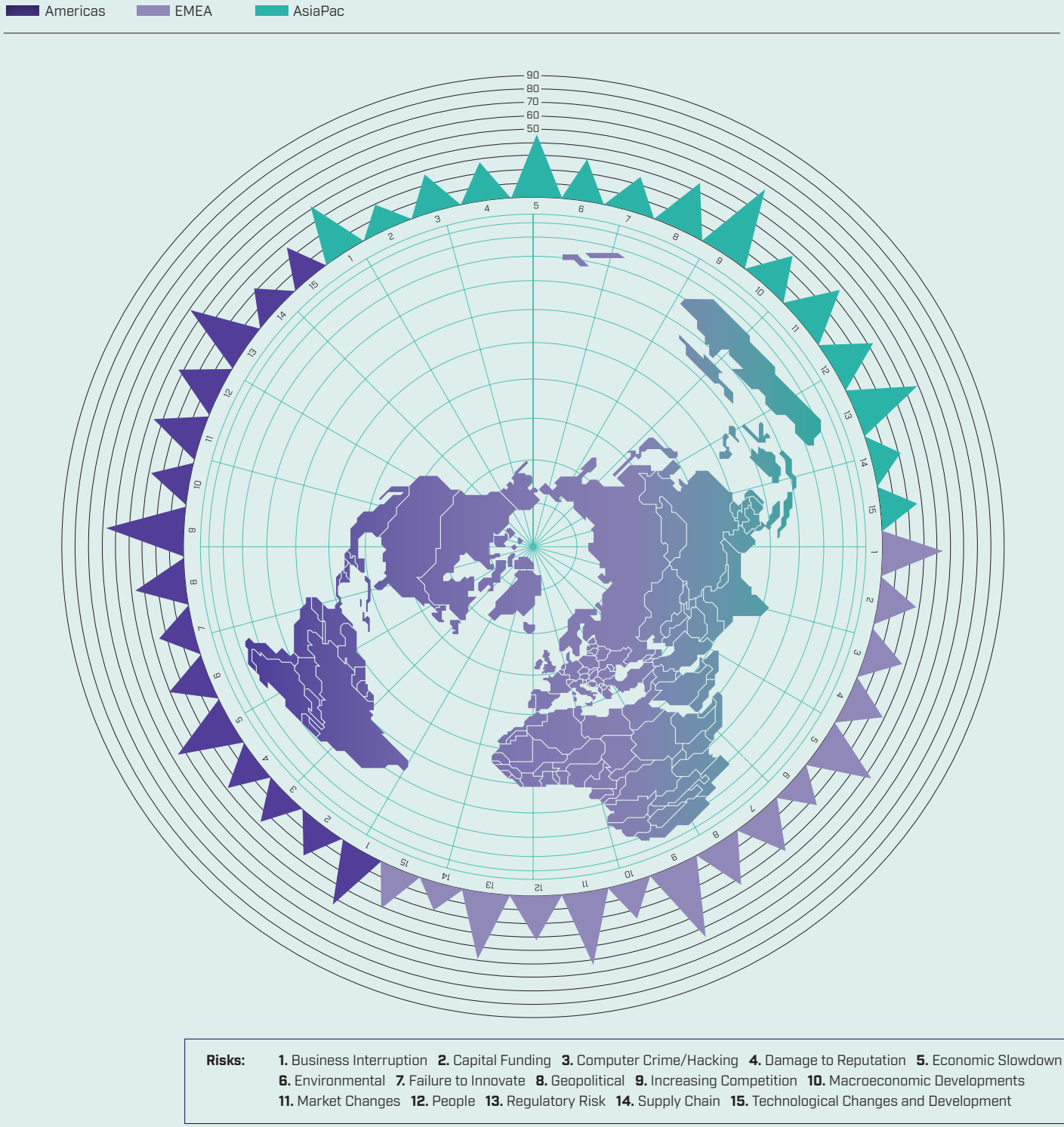
For companies, the stricter environment creates new exposures and a higher cost of compliance. This is clearly reflected in the survey findings. Perhaps unsurprisingly, it is most keenly felt by organisations in the Americas and Europe, the Middle East and Africa, which have been most affected by the aftermath of the 2008 crisis.

Not only are country-level supervisors stepping up their enforcement action, there has also been more international co-operation between regulators. For companies that have business dealings in the US, for instance, regulators such as the Securities and Exchange Commission have proved to have a very long arm. This has particularly been the case when implementing the Foreign Corrupt Practices Act.

Half of all respondents point to regulatory risk as the main threat to their business currently, with the largest organisations (with revenues over $5 billion) and smallest (with revenues under $500 million) considering this a greater concern. This possibly reflects the difficulty large multinationals have navigating legislation across multiple regions, and the challenge to smaller organisations of dealing with the cost of compliance.

Regulation is also deemed the risk that has affected survey respondents most over the last three years. Looking forward, it is considered the second-biggest risk over the coming decade. “Businesses in the financial sector around the globe have all been quite heavily impacted by regulation

FIGURE 3. Which risks, if managed well, do you believe will increase the value of and results for your organisation?



Risks: **1.** Business Interruption **2.** Capital Funding **3.** Computer Crime/Hacking **4.** Damage to Reputation **5.** Economic Slowdown **6.** Environmental **7.** Failure to Innovate **8.** Geopolitical **9.** Increasing Competition **10.** Macroeconomic Developments **11.** Market Changes **12.** People **13.** Regulatory Risk **14.** Supply Chain **15.** Technological Changes and Development

in order to recapitalise the banking sector," says Nigel Burbidge, Partner / Global Chair Risk & Advisory Services at BDO. "Regulators are also a lot more joined up and have greater resources at their disposal."

But where there is risk there is also opportunity. Fifty-three per cent of respondents recognise that managing regulatory risk well would add value to their business. By instilling effective checks and controls, such as governance and environmental resources management frameworks, organisations are less likely to fall foul of laws in the countries in which they operate – and hence run a better business.

Risk in a joined-up world

The increasing digitalisation of the business environment is both a risk and opportunity for the future. Respondents identified technological changes and development as the fourth most impactful macro risk trend over the coming decade, with 36 per cent believing the ability to manage such risks would

FIFTY-THREE PER CENT OF RESPONDENTS RECOGNISE THAT MANAGING REGULATORY RISK WELL WOULD ADD VALUE TO THEIR BUSINESS

add significant value to their business.

"The world is much more complicated," says Julia Graham, technical director at Airmic, the risk managers' association. "One of the reasons it is more complicated is that innovations like the internet of things (IoT) are connecting everything, whether it's your refrigerator or a driverless car or a drone."

The IoT has great potential to reduce risk in many areas of our lives. Telematics in cars is just one example, with the technology helping to improve driving behaviour by capturing data and offering feedback. Likewise, the connected home has the ability to alert homeowners to flood, fire and intruders, among other things. And while it is early days with wearable device technology, in the future the opportunity to spot indicators of disease should allow much earlier medical intervention.

But in a world where 20 billion devices could soon be wirelessly connected to the internet (as a recent study by Gartner predicts would be the case by 2020, rising from six billion this year), there are also new risks to consider. One is simply failure to innovate and seize the opportunity IoT offers. Another is cyber risk and data exploitation.

"The issue you're going to increasingly have is when you connect things to the internet, then potentially, with the right technology and sophistication, that system is going to be accessible to anyone," explains Beazley cyber underwriter Jimaan Sane. "There are advantages to connecting things to the internet – because then you can gather information or send commands remotely. So in your car, home or office it's very useful and there are lots of advantages and features that you can draw from it. But also there are going to be some security challenges."

RACONTEUR

CUSTOM PUBLISHING