RESPONDING TO GLOBAL RISKS

A practical guide for business leaders

2014

Airmic

Airmic represents corporate risk managers and insurance buyers. Its membership includes two-thirds of the FTSE 100, as well as many smaller companies. The association organises training for its members, seminars, breakfast meetings and social occasions. It regularly commissions research and its annual conference is the leading risk management event in the UK. In 2014 it published the risk management report *Roads to Resilience*.

Marsh

Marsh is a global leader in insurance broking and risk management, with approximately 27,000 colleagues working together to serve clients in more than 100 countries. Marsh helps businesses around the world to succeed by defining, designing, and delivering innovative industry-specific solutions that enable them to manage risk effectively. Marsh is a wholly-owned subsidiary of Marsh & McLennan Companies.

PwC

As the UK's leading provider of integrated governance, risk and regulatory compliance services, PwC specialises in helping businesses and their boards create value in a turbulent world. Drawing from a global network of specialists in risk, regulation, people, operations and technology, PwC helps its clients to capitalise on opportunities, navigate risks and deliver lasting change through the creation of a risk-resilient business culture.

Zurich

Zurich Insurance Group is a leading multi-line insurer serving customers in global and local markets. With more than 55,000 employees, it provides a wide range of general insurance and life insurance products and services. Zurich's customers include individuals and businesses of all sizes, including multinationals, in more than 170 countries. The Group is headquartered in Zurich, Switzerland, where it was founded in 1872.

Institute of Directors

The IoD is the leading organisation supporting and representing business leaders in the UK and internationally. One of its key objectives is to raise the professional standards of directors and boards, helping them attain high levels of expertise and effectiveness by improving their knowledge and skills. It is the publisher of *Business Risk: a practical guide for board members*, also produced in collaboration with Airmic and PwC.

RESPONDING TO GLOBAL RISKS

Practical advice for business leaders

2014

Group Editor, Director Publications Ltd: Lysanne Currie
Consultant Editor: Tom Nash
Creative Director: Chris Rowe
Production Manager: Lisa Robertson
Head of Commercial Relations: Nicola Morris
Director General: Simon Walker

Published for the Institute of Directors, Airmic, Marsh, PwC and Zurich
by Director Publications Ltd, 116 Pall Mall, London SW1Y 5ED
020 7766 8910
www.iod.com

A CIP record for this book is available from the British Library
ISBN 978-1904520-86-3
Printed and bound in Great Britain

The Institute of Directors, Airmic, Marsh, PwC, Zurich and Director Publications Ltd accept no responsibility for the views expressed by contributors to this publication. Readers should consult their advisers before acting on any issue raised.

Contents

Part 1: Introduction

Part 2: Addressing critical impacts

Part 3: Board responses

Foreword

Simon Walker

Director General,
Institute of Directors

The catalyst for this guide has been the latest annual report on global risks from the World Economic Forum (WEF). We make no apology for referencing this excellent study because it provides vital insights into how industry leaders and experts perceive evolving, interconnected risks that cut across national boundaries, the economy, technology, society, and the environment.

The WEF's *Global Risks 2014* report analyses 31 global risks over the coming decade. The risks are grouped under five classifications – economic, environmental, geopolitical, societal and technological – and measured in terms of their likelihood and potential impact.

The 10 risks of highest concern to respondents are:

1. Fiscal crises in key economies
2. Structurally high unemployment/underemployment
3. Water crises
4. Severe income disparity
5. Failure of climate change mitigation and adaptation
6. Greater incidence of extreme weather events
7. Global governance failure
8. Food crises
9. Failure of a major financial mechanism/institution
10. Profound political and social instability.

Of these threats, income disparity, extreme weather events and unemployment/underemployment are the three most likely to cause major cross-border damage in the next 10 years. Fresh fiscal crises, climate change and water shortages, although seen as less likely, are the three that would have the largest global impact. Further, the study describes the coalescence of various global risks into three unwelcome scenarios: a 'generation lost' because of social and economic strains on young people; 'digital disintegration' due to the world's increasing reliance on the internet despite its vulnerabilities; and 'instability in an increasingly multipolar world' from rising geopolitical tensions.

WEF's study highlights how global risks are not only interconnected, but also have systemic impacts. It concludes that greater effort is needed to manage them effectively.

And that is where this guide comes in. It is one thing to analyse global risks but, in the absence of a global authority to control them, it falls to organisations, boards and individual leaders to understand their impacts and build resilience to them at both a strategic and operational level.

This is by no means negative thinking. Improved resilience breeds increased confidence, greater enterprise and other benefits. Equally positive is the reality that a threat to one organisation can be an opportunity for another. A constant theme of this guide is that businesses can achieve competitive advantage through an effective response to global risks.

Written by leading experts, the following chapters will help IoD members and other leaders, in both large and small organisations, understand how interdependencies between risks evolve, offering them fresh thinking and practical advice to supplement traditional risk management tools.

> “Improved resilience breeds increased confidence, greater enterprise and other benefits”

Chapter 1

Managing global risks

To achieve a company's strategic objectives, the board must decide what risks it is willing to take. This task is particularly challenging when it comes to assessing global risks.

Dr Roger Barker

Director of Corporate Governance and Professional Standards, Institute of Directors

Although risk management may sometimes appear to be the province of specialist risk managers, it is increasingly recognised that the board of directors must play a central role in managing risks. For example, the UK Corporate Governance Code states: "The board is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems". But boards typically find that global risks – which are the focus of this publication – are tricky both to conceptualise and manage. One of the lessons of the recent financial crisis was that companies often focus too much on their own company-specific risks and not enough on overarching systemic risks.

Such risks tend to originate beyond the normal activities of the company, and the board may feel that it lacks sufficient in-house know-how to fully understand their causes and business implications. And yet such risks have the potential to exert a huge impact on the company's success or failure, both at an operational level and, often more importantly, in terms of its overall business strategy. Equally, they can give rise to a range of business opportunities that, if successfully exploited, can translate into a major source of competitive advantage. One company's nemesis may be another's reason to exist.

Since 2006, the World Economic Forum (WEF) has published its annual *Global Risks* report. This widely-referenced study provides a unique insight into the significant and emerging risks that are seen as most likely to bring calamity or opportunity to a wide range of organisations. It provides the starting point for the rest of this publication, which seeks to offer practical guidance to businesses on how they might respond to the impact of these global risks.

According to the WEF report, a global risk is defined as an occurrence that causes significant negative impact across many countries, industries and organisations over a sustained period of time (up to 10 years). Such risks may be economic, environmental, geopolitical, societal or technological in origin. Their common characteristic, however, is their potentially systemic impact – they not only affect individual organisations but may also give rise to a contagion effect that can generate disruptive shockwaves across entire economic, societal, environmental, technological and other systems.

Although such global risks may seem to be less immediate than more organisationally-specific risks, their commercial impact is potentially just as real. Unlike other risks to the business, their effects are likely to be difficult to avoid due to their wide-ranging systemic nature. Consequently, boards must develop a framework of decision-making, oversight and embedded values that enables this kind of risk to be managed.

Most governance frameworks break down the board's risk oversight responsibilities into distinct components, each of which is relevant to the management of global risks:

- Determining the organisation's desired trade-off between risk and reward. This typically involves defining the risk tolerance (or appetite) of the enterprise, which in turn guides the development of the business strategy. In other words, what sort of activities does the organisation wish to undertake and which will it avoid?
- Identifying and reviewing the portfolio of risks to which the organisation is exposed, and determining whether to accept, avoid, manage or outsource them. Risk is a fact of life, but the board has a choice about how to deal with it.
- Monitoring management's efforts to maintain effective risk management and control systems, and ensuring that relevant risk policies and values are fully applied.
- Communicating to shareholders and other stakeholders the critical risks faced by the organisation, and providing assurance that they are being well managed. Boards not only have to ensure that risks are managed effectively; they must be seen to be managed in an appropriate way.

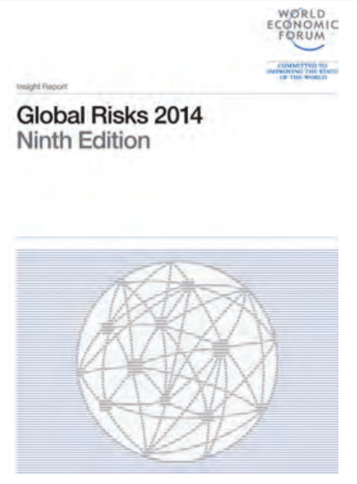
Snapshot

- It is a key task for the board to perform ongoing risk oversight. It can't be delegated to risk management specialists.
- Boards typically find that global risks, though potentially catastrophic, are difficult to conceptualise and manage.
- Boards play a pivotal role in defining the company's risk appetite and in identifying major global risks.
- There is a need to create culture of risk awareness and build resilience into the business.

> "Global risks have the potential to exert a huge impact on the company's success or failure"

In large organisations, many aspects of the board's role will involve risk oversight rather than risk management (which will be undertaken by the CEO and executive team), whereas in smaller companies the board may play a more 'hands on' management role, both in the identification of critical global risks and the direct operation of risk management systems.

But even in the largest corporations, which may employ significant numbers of risk management specialists, the board will typically be well placed to play a key role in the assessment and oversight of global risks and their impacts. The strategic importance of global risks means that they are an essential aspect of board-level discussions of the corporate vision and business model. And the board is a better vantage point than elsewhere to take a broad view of the organisation and its business environment, bringing to bear the wide-ranging experience of both executive and non-executive board members. For this reason, oversight of global risks is not something that can be mainly delegated to specialist risk managers or in-house internal control functions. It demands a board-level perspective. In some cases, it merits the board-level role of chief risk officer (CRO) – with the key task of identifying links between global risks and organisational impacts, ensuring resilience.



A commonly-utilised tool in the board's risk oversight process is the risk register, which classifies individual risks in terms of their likelihood and impact and identifies measures for mitigating them. The risk register may also specify a manager or board member who is personally accountable for the management or oversight of the particular risk. In addition to regular board meetings, boards may also use strategic 'away days' to brainstorm such risks in more detail, incorporating the input of both management and external experts.

Some global risks may be 'slow-burn', but a lesson of recent corporate crises is that many are sudden and difficult to identify in advance. Furthermore, interrelationships between different types of risk mean that analysing them individually may lead to seriously misleading conclusions.

It is also important that the board builds sufficient resilience into its business model and operational processes, in order to support the organisation in coping with the impact of a variety of global risk outcomes, including the so-called 'black swan' events that are not widely anticipated. Appropriate precautions, many of which are discussed in this Guide, include business continuity arrangements, securing emergency access to human, financial and physical resources, and ensuring adequate margins of error in the design of technical and operational systems.

Tooling up

In a ground-breaking article, Managing Risks: A New Framework, (*Harvard Business Review*, June 2012), Harvard professors Robert Kaplan and Annette Mikes highlight the importance of using appropriate tools for different types of risk management.

Kaplan and Mikes argue, "Despite all the rhetoric and money invested in it, risk management is too often treated as a compliance issue that can be solved by drawing up lots of rules and making sure that all employees follow them. But rules-based risk management will not diminish either the likelihood or the impact of a disaster such as Deepwater Horizon, just as it did not prevent the failure of many financial institutions during the 2007–2008 credit crisis."

They present a new categorisation of risk that allows businesses to tell which risks can be managed through a rules-based model and which require alternative approaches. Their category of 'external risks' includes global risks such as natural and political disasters and major macroeconomic shifts. "Because organisations cannot prevent such events from occurring, they must focus on identification and mitigation of their impact," they say.

To link global risks to business impact, boards need to use tools such as scenario planning. In this way risk management at board level becomes closely aligned with the strategy process. This is a very different risk tool suite to the preventative risk models that might be employed to quantify 'hygiene factor' operational risks such as health and safety risks, or 'value at risk' (VaR) for financial product mark-to-market risk evaluation.

In larger organisations, the board may delegate certain aspects of its risk oversight responsibilities to board committees. Traditionally, the audit committee has been a forum for this kind of additional scrutiny, but an increasing trend – particularly in financial institutions – is for a designated risk committee, and the associated executive and board-level role of CRO, to be created. This may permit more attention to be paid to emerging risks, beyond the more backward-oriented issues of financial reporting, audit and control that can absorb the audit committee.

Although an effective board will seek to play a crucial role in the governance of risk, directors should be conscious of the need for a strong risk-aware culture throughout the organisation. The board faces a particular challenge in large and complex organisations, where it must find ways to encourage employees at all levels either to address potential risks themselves or flag them up to leaders without delay or fear of the consequences.

But for this to happen, the board must nurture a 'no blame' culture, particularly in terms of its own relationship with the CEO (which, if it breaks down, poses a critical but often unacknowledged risk for the organisation), but also through the establishment of reliable lines of communication between the board and other employees involved in risk management activities, including whistleblowers. The board needs to engender a healthy level of trust between itself, management and employees to avoid the creation of a 'risk management glass ceiling' between the board and the rest of the organisation.

Effective boards will also wish to increase their ability to manage global risks by encouraging diverse and challenging perspectives within the boardroom itself. This will include: considering how diversity can be achieved on the board; recognising the limits of their own direct oversight capacities; and searching for ways to embed and incentivise appropriate ethical behaviours throughout the organisation. And they might consider how the redesign of organisational structure could simplify the board's oversight of the business and facilitate easy communication between all levels of staff.

Ultimately, it is the board that is responsible for the governance of risk. But given the uncertainty and potential impact of the global risks highlighted by the WEF report, it is the people and culture of the entire corporate entity that will determine if these risks can be successfully navigated.

> “The board must find ways to encourage employees at all levels either to address potential risks themselves or flag them up”

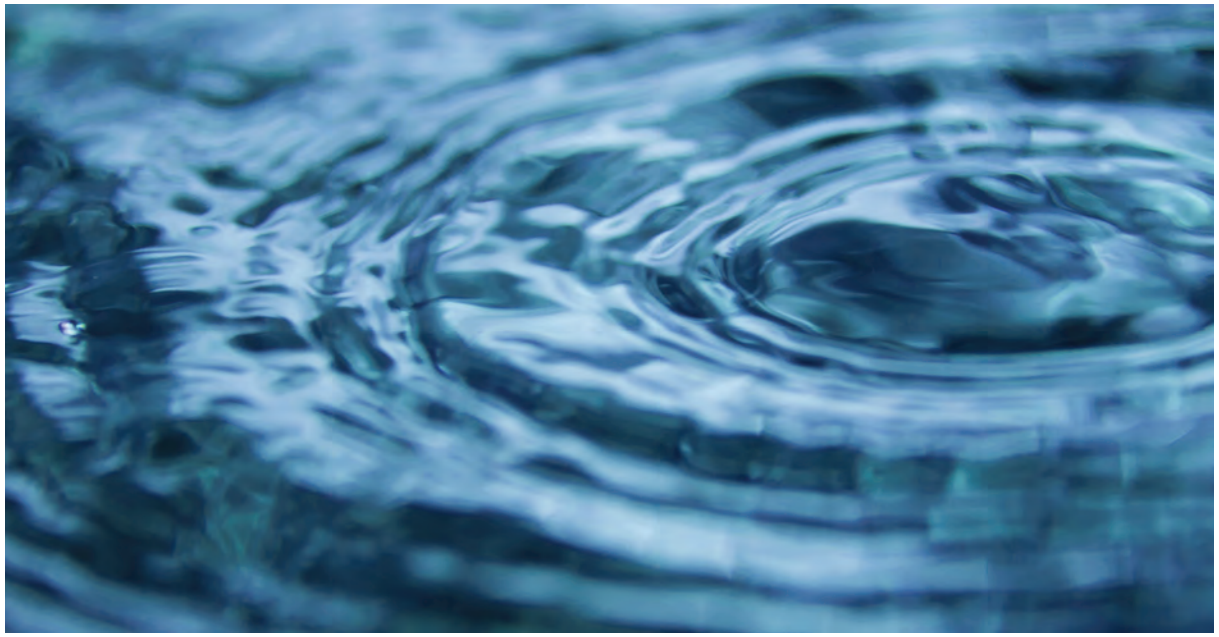
Checklist for the board

- Do we have a framework of decision-making and risk oversight that fully incorporates evaluation and management of global risks?
- Does the board devote sufficient time and resources to the evaluation of global risks?
- Should we appoint a chief risk officer or form a dedicated risk committee?
- Have we evaluated the potential impact of today's global risks and drawn up a risk register?
- What can we do to instil a culture of risk awareness and build resilience into our business model and operational processes?

Chapter 2

Risks carry consequences

Businesses face a plethora of global risks, placing the onus on boards to recognise them and take steps to mitigate them. It is a daunting task, but not an impossible one.



John Scott

Chief Risk Officer, Zurich Global Corporate at Zurich Insurance Group

Over 30 global risks are described in the WEF's *Global Risks 2014* report. They cover significant issues ranging from environmental risks such as climate change and severe weather to societal changes such as longevity and social disparity. Macroeconomic risks such as fiscal crises, with their consequences including fiscal austerity, currency wars and asset bubbles, are particularly important in terms of their interconnectedness and impact on other risks.

It is easy for individuals and organisations to feel overwhelmed by the enormity of this global risk landscape. The implications of global risks on an individual or business scale can appear difficult to discern and often remote from day-to-day challenges. But nothing could be further from the truth. In our globally connected world, even the most local businesses are dependent on global events in ways they could never have dreamed of just a few years ago. While it is not easy for an individual to change the likelihood or impact of any one global risk, it is perfectly possible to think through the consequences of global risks for any business and to take steps to mitigate them. Indeed, many very different risks can have similar consequences.

It is the interconnected and systemic nature of global risks that creates surprises when their impacts are felt locally. Human beings are generally poor at putting risks into context, especially the probability component. People often don't take into account extremes in probability distributions. Somehow it seems safe to get into your car and drive home, even though statistically you are far more likely to die in your car than anywhere else. Similarly many people buy lottery tickets in the hope and expectation that 'it could be me' even though you are about as likely to be hit by lightning as win the big one.

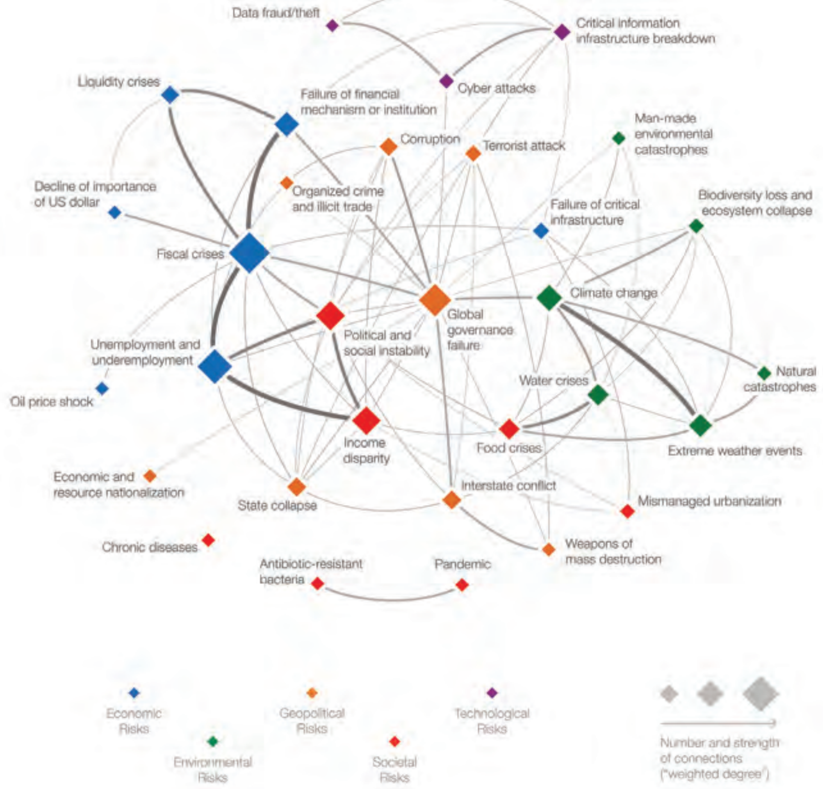
So against this complex background of interconnected and systemic global risks, it is important for businesses to understand the triggers, trends and scenarios to look out for and to prepare for the consequences they may have to face.

There are a handful of generic consequences of global risks that are common to most organisations. 'Fiscal crises' is rated as the highest-impact global risk in 2014. We are still living with the consequences of the 2008 fiscal crisis and there are strong interdependencies with other global risks including failure of a financial mechanism or institution, liquidity crises, unemployment and underemployment, political and social instability and income disparity. The impact on individual businesses of economic downturns has implications for companies' corporate and competitive strategies.

Snapshot

- Over 30 global risks are described in the WEF's *Global Risks 2014* report, many of which are systemic and interconnected.
- It is important for businesses to understand the triggers, trends and scenarios to look out for, and to prepare for the possible consequences of risks.
- There are a handful of generic consequences of global risks that are common to most organisations.
- Global risk management is part of good corporate governance and, as such, should embrace sustainability principles.

Global Risks 2014 Interconnections Map


Data fraud/theft
Critical information infrastructure breakdown
Liquidity crises
Cyber attacks
Failure of financial mechanism or institution
Corruption
Terrorist attack
Man-made environmental catastrophes
Decline of importance of US dollar
Organized crime and illicit trade
Failure of critical infrastructure
Biodiversity loss and ecosystem collapse
Fiscal crises
Climate change
Global governance failure
Political and social instability
Unemployment and underemployment
Water crises
Natural catastrophes
Oil price shock
Income disparity
Food crises
Extreme weather events
Economic and resource nationalization
State collapse
Interstate conflict
Mismanaged urbanization
Chronic diseases
Weapons of mass destruction
Antibiotic-resistant bacteria
Pandemic
Economic Risks
Environmental Risks
Geopolitical Risks
Societal Risks
Technological Risks
Number and strength of connections ("weighted degree")

Source: *Global Risks 2014*, World Economic Forum, Switzerland.

Difficulty to access trade credit, or other forms of longer-term financing can have immediate impact on credit ratings and the ability to survive let alone thrive in such a tough economic environment. Firms may have to implement immediate cost-reduction exercises, look to new sources of funding and explore new markets, but planning for such eventualities can mitigate this. Maintaining healthy cash balances and not losing focus on a lean cost structure, not to mention some strategic planning, can help in such circumstances. It is noticeable that economic downturns are also opportunities when the strongest and most prepared survive at the expense of their weaker competitors.

Extreme weather events are rated as the second most likely global risk in 2014, behind income disparity. Other environmental risks also rate highly, from water crises, failure of climate change mitigation and adaptation to the consequences of natural catastrophes (earthquakes, tsunamis, volcanic eruptions and geomagnetic storms). These events typically have significant effects on supply chain interruption. No matter the size, scope or scale of a company, the chances are that in our globalised world there are components or supplies which are sourced from remote locations, often many thousands of miles away in low-cost manufacturing economies. Some of these interruptions can be on the level of a nuisance, but some can effectively bankrupt an individual organisation. This is especially so when lower working capital targets and just-in-time manufacturing philosophies have limited supply chain flexibility and reduced supply chain resilience. Looking to simple strategies to localise supplies, develop multiple suppliers and design-in product and service flexibility can help mitigate these impacts

Driven in part by the global fiscal crisis, the global risk of unemployment and underemployment links strongly with other risks including political and social instability income disparity. Youth unemployment rates have soared since the financial crisis. The situation is especially dire in the Middle East and advanced economies, notably some European countries such as Spain and Greece. About 300 million young people – over 25% of the world's youth population – have no productive work, according to World Bank estimates. Prospects for the young generation are brighter in high-growth markets, particularly in Asia, where the middle-classes are rising. The developing economies of China, Latin America and Africa face additional pressures of population growth as rural-urban migration creates megacities with complex risks and vulnerabilities. Companies operating in either developed or developing economies need to develop human resource strategies to deal with the situation. Apprenticeship schemes in areas of low youth employment can build a skilled and committed workforce. In the emerging markets, jobs abound while the broad-based skill sets required for a well-diversified workforce have yet to catch up. Companies must engage young people now, often in partnership with Government, to discuss practical solutions on their terms, with the power to create fit-for-purpose educational systems, functional job markets, efficient skills exchanges and the sustainable future on which we all depend.

Geopolitical friction

As the floodwaters of the financial crisis recede, the fault lines in global governance appear to have widened.

Debt-laden advanced economies are reluctant to cohere on costly foreign policy initiatives and are prioritising those offering short-term national advantage. Large emerging markets want to flex their muscles on the international stage, but face increasing pressure from citizens at home for far-reaching economic, social and political reform. Not only is this triggering and exacerbating geopolitical friction, it is also inhibiting the development of solutions to long-term global challenges. The diversity of viewpoints has made it increasingly hard for multilateral institutions to achieve authoritative consensus between stakeholders.

Recent unrest in Turkey, Brazil and South Africa is a sharp reminder of the challenges to achieving stable economic growth, and the importance of effective governance. The unresolved crisis in Syria threatens progress in the Middle East. Relations between some of the leading Asian economies have deteriorated. The situation in Ukraine risks a fresh rupture between East and West.

These corrections to the course of globalisation and global development create a highly uncertain environment for critical sectors (such as energy) and businesses in general. Companies should anticipate shocks, setbacks and policy reversals in markets undergoing significant change. They may want to enhance their strategic agility and hedge their exposure to at-risk economies. Geopolitical volatility is likely to be a key driver of uncertainty over the next few years.

Cyber risks have been a focus of successive *Global Risks* reports by the WEF. These range from failure of critical information infrastructure, to the risks of digital wildfires, spreading misinformation through social media. In 2014 the focus shifted to the threats of digital disintegration, a loss of trust in an internet that is subject to constant attacks from criminals and 'hacktivists' and increasingly used for espionage and warfare by state actors. This has significant impact on individual firms in their management of data privacy and security. No longer the responsibility of the IT manager, or IT security specialist, this is now a topic for the boardroom, as new business models are being challenged and customers or employees expect their personal data to be kept secure. This requires not only a good understanding of digital strategies, but also of physical security – from 'clean desk' policies in the workplace to employee vetting procedures for staff handling critical or sensitive information in whatever format. Governments are now beginning to wake up to the importance of working with the private sector to raise awareness and share information about the source of cyber attacks. It is every business's responsibility, whether large or small to understand the impact on its particular business model and know how to respond, even with the simplest of physical security responses.

In all the consequences of these global risks lies one risk for companies that results from their inability to discern the local impact – and that is reputation risk. Increasingly, resilience to the consequences of global risks is no longer seen as something to be left to chance. Indeed in regulated industries, regulators are beginning to demand that firms show evidence of a risk management culture and that they not only follow the rules, but also do the right thing. The implications for corporate governance and the ethical dilemmas many employees face goes to the heart of a firm's 'moral purpose', ie. what an organisation exists to do. No longer is it acceptable for a bank to be seen to exist to pay high remuneration to its staff rather than to provide capital to invest in a growing economy. The management of the consequences of global risks is just one aspect of this fundamental aspect of board leadership and good governance.

> “
> Increasingly, resilience to the consequences of global risks is no longer seen as something to be left to chance”

Checklist for the board

- Have we accepted our business's vulnerability to global risks and our obligation to manage them?
- Have we reviewed the critical global risks identified in the WEF's *Global Risks 2014* report and recognised their systemic and interconnected nature?
- Have we considered the potential impact of these risks on our business, including the risk to our reputation?
- What steps have we taken to create a risk management culture? (See chapter 1).
- Do we acknowledge that this culture should have an ethical dimension, embracing our organisation's moral purpose, as well as its need to survive and prosper?

Chapter 3

Financial fractures

Businesses inhabit a harsh post-crisis world when it comes to accessing finance and managing the associated risks. But opportunity may be the reward for vigilance.

James Sproule

Chief Economist and Director of Policy at the Institute of Directors

Risk and reward – or fear and greed if you prefer – are opposite sides of the same coin, and always will be. That said, perceptions of risk generally, and even more obviously global financial risk, have changed beyond all recognition in recent years.

In particular, greater amounts of data and increased computing capacity have allowed many measures of risk to move from the theoretical to the practical, making risk easier to measure than has ever been the case before.

Furthermore, the scope of risk has expanded. Along with credit and market risk, businesses must now also consider liquidity, counterparty and systemic risk.

The credit crisis meant that many a company and even banks, whose understanding of financial risk had hitherto been considered well developed, found that models have their limits. The arsenal of quantitative risk management tools are no substitute for informed qualitative judgements and experience. Understanding individual risks is not enough; we must ensure that remote possibilities and risk interdependencies are also taken into account. Time and again, financial instruments that promised to be 'insurance' against one or another danger came apart under pressure. Counterparties who had been thought to be completely trustworthy, and financial instruments that had always previously been highly liquid, proved to be the opposite. Many assumptions were tested to destruction, and an important concept in financial risk management was affirmed: no matter how sophisticated the process of slicing and dicing risk, it does not go away. Ultimately someone still holds the risk.

What has become clear is that global financial risk is going through a period of dynamic change. This leaves what was always an amorphous concept even more difficult to define and equally challenging to price.

For banks, there has been a reassessment of the nature of global financial risk, with regulators leading the way in demanding greater capitalisation, and banks themselves responding by consolidating balance sheets and generally raising the cost of finance for businesses. This was a long overdue and predictable first stage of reassessing risk. Yet as banks have reduced their risk, investors have regained confidence and they are once again searching for yield, and naturally as a part of that, accepting risk. A shadow bank or fund structure (call it what you will), where frequent reassessments of risk and resulting valuations simply alter the value of a fund, as opposed to such revaluations triggering a requirement for fresh capital, may well be more appropriate for the business world we are moving towards.

Looking beyond the effect of changing risk assessments for banks, four factors in particular have left businesses more vulnerable to global financial risk:

- As global markets have expanded, so too have the myriad interconnections between economies and businesses, leading to a host of unforeseen circumstances. Who would have anticipated that the failure of instruments 'as safe as houses' would be the harbinger of a global crisis? Or that banks on the other side of the world would be so exposed to instruments they did not actually understand? Or that sovereign bonds, or 'risk-free assets' as they were often termed, would prove to be quite so vulnerable and volatile? In truth, the history of sovereign bond defaults is littered with examples of investors losing their money, so the idea of 'risk-free' returns from this asset class has never been sound, except for the central bank gilts of the most stable economies. The lesson of the most recent financial crisis is that even the most stable economies are subject to volatility. Despite the hubris of some pre-crisis politicians, who were quick to claim "no more boom and bust" during the period of credit growth in the early 2000s, businesses should always remain aware of the underlying risks in a global 'macroeconomy' and adjust their business models to take

Snapshot

- In the wake of the global financial crisis, businesses remain vulnerable to financial risks.
- Boards should appreciate the potential volatility of markets and fluctuating valuations, and should ensure that financial risks are continually monitored.
- But businesses should not be obsessed with downside risks and should remain open to potential opportunities.

“The credit crisis meant that many a company, and even banks, found their models wanting” these into account. As all business people know, there is no reward without risk, but it is the prudent business that understands the risks and takes advantage of volatility. Ultimately, individual businesses may fail and there is a strong argument that no business should be too big to fail.

- More and more parts of the economy have been 'monetised'. In the past, a company might well have owned many of its premises and, while the value of those premises may have fluctuated, the effects of this were minimal as all the balance sheet showed was a constant, conservative book value. Today, businesses' premises are invariably leased, with the lease itself being traded and potentially used as collateral in a variety of financial transactions. In these circumstances, any fluctuation in the perceived value of the premises and the lease has a ripple effect across the economy that did not exist even 20 years ago.
- In general, businesses, banks, governments and households became too dependent upon under-priced capital. High degrees of leverage mean that even modest declines in growth expectations rapidly demand drastic action. The ultra-easy credit conditions, which ran for a decade prior to the 2007 crunch, lulled many into the naïve assumption that the good times would continue *ad infinitum*.
- Finally, there has been a proliferation of financial derivatives that, in the credit crisis, did not prove as resilient as promised. In practice, the ultimate risks of many of the more bespoke instruments, and those such as credit default swaps, proved hard to discern and have become much less popular in the market as instruments to transfer financial risk. Although credit default swaps are still available, and are a good measure of an individual company's credit strength, investors are now much more keenly aware of what they do and what they represent. A hard truth has been driven home: a derivative, whilst promising enhanced returns, can concurrently expose the holder to increased risks.

Eurozone stagnation

In the aftermath of the credit crisis, the Eurozone has had a series of difficulties. In particular, European banks used sovereign bonds as a part of their core capital and, as the viability of continuing deficit financing has been questioned, banks' solvency has in turn been scrutinised.

At the same time, citizens of the southern states of the Eurozone have moved a substantial proportion of their savings to northern EU banks, leaving local lenders with diminished balance sheets. The result is that credit has all but evaporated: after expanding by an average annual rate of 7% in the decade before 2007, the increase is now less than 2% a year. And that is an average across the Eurozone. In southern Europe, where credit has been shrinking, an early economic recovery looks unlikely.

From riches to rags

Following a spate of acquisitions, Premier Foods became the UK's largest food company in 2006, employing around 20,000 staff and providing a home to some famous food brands, such as Hovis, Homepride, Oxo and Mr Kipling. But by the end of 2013, it was being described in the media as a 'zombie' company, with most of its cashflow absorbed by debt servicing payments and the financing of a significant pension fund deficit.

How did Premier move from riches to rags in the space of just a few short years? Although debt-fuelled acquisitions – particularly the takeover of Ranks Hovis McDougall in 2007 – placed Premier in a vulnerable position, its fortunes were sealed by two global market developments. The first was a significant increase between 2005 and 2008 in the global price of wheat, which dramatically reduced Premier's profit margins. The second was the advent of the global economic downturn after the financial crisis of 2007/2008, which pushed down sales of its products in its major markets. In addition, a complex financial hedge, designed to protect against rising interest rates, proved costly to unwind when rates moved downwards in the wake of the financial crisis.

Since 2007, Premier has undergone four separate restructurings, shed 11,000 staff and sold many of its famous brands. In 2010, market capitalisation declined below £100m (from a high of more than £2bn) as investors priced in the possibility of insolvency. Current CEO, Gavin Darby, believes the worst is now behind the company, but it still faces major challenges if it is to rebuild its financial position and its reputation.

Pensions timebomb

That there is a risk involved in any long-term financial arrangement is obvious, and there are few arrangements as long-term as pensions. Famously, a poll once asked American teenagers if they believed in alien life on another planet, and also if they thought they were likely to receive a retirement income from the US social security system. The answers were 'yes' to the first and 'no' to the second, showing that American youth has a good grasp of the realities of long-term risk.

Estimates vary, but total unfunded pensions liabilities could easily double the UK's debt-to-GDP to more than 200%. At this level, the risk is not merely that pensions liabilities could cause trouble for companies, as they have already for firms such as British Airways, but that the risk transmutes from 'corporate' to 'individual'. Government promises will be rewritten and laws enacted to allow companies to reschedule. The risk is not that companies or governments will be brought down by pensions liabilities, but that promises will simply not be honoured.

The process of financial fracture we have been through has highlighted the importance to business of continual monitoring of global financial risks. Whilst not obsessing over this task, boards should appreciate that all valuations are dynamic.

But the post-crisis world also offers opportunities. Many of the worst excesses of the credit boom have now been addressed and banks are in far better shape than they were in 2007 (would that the same could be said about government finances). Banks' capital reserves have largely been rebuilt and they are now beginning to expand their lending, as opposed to their recent practice of closing credit lines to even the most solvent and longstanding of clients.

What is not going to happen is a return to 'covenant light' lending, essentially lending with few risk controls. Banks will vary in how they approach lending, decentralise decision-making and assess risk and the companies they lend to. The implication for businesses is that it will pay to shop around to find the banks that want you as much as you want them. After all, it is not as if there is any difference in the final 'product' they are lending you!

> “Many of the worst excesses of the credit expansion have now been addressed, and banks are in far better shape today than they were in 2007”

Checklist for the board

- The best form of 'insurance' is agility. How much extra would avoiding being tied into long-term contracts really cost? Is that a cost it would be sensible to accept?
- Robust scenario planning should include driver analysis that takes into account 'large impact but small likelihood' events. But remember to review scenarios for the opportunities, as well as the downside risks, each may bring.
- Avoid financial instruments you do not fully understand. If they cannot be quickly and comprehensively explained to you, including all of the potential risks, it would be wise not to invest.
- Shop around. Banks are open for business again, but they have very different business models and methods of assessing risk. Find the bank that appreciates and suits your business.

Chapter 4

Logistical nightmares

In a connected, globalised economy, disruptive incidents can often have repercussions for infrastructure and supply chains that are felt on the other side of the world.

Caroline Woolley

EMEA Property Practice Leader and Global Business Interruption Centre of Excellence Leader, Marsh

The recurrent theme of the WEF's *Global Risks 2014* report is global events that impact upon businesses of all sizes. From natural catastrophes such as earthquakes and floods to man-made mayhem in financial markets or cyberspace, in a hyperconnected, globalised economy, incidents often have repercussions for global supply chains that can be felt on the other side of the planet.

Complex supply chain liabilities were infamously exposed in 2011 in the aftermath of Japan's Tōhoku earthquake and resulting tsunami, and again later that year by the Thai floods. The impact of these two incidents on automotive manufacturing and hard disk drive production respectively was dramatic, and revealed the limited information on full supply chains and aggregated supplier risk.

Since then, companies have invested large amounts of money into trying to improve their understanding of supply chain risk, as they have sought to build resilience into their business and gain competitive advantage over rivals. However, as supply chains have become longer and more complex, so the opportunity for failure at any critical point is greater than ever before. Supply chain exposures are changing as well, and today virtually all of the macro issues at the heart of the WEF report present heightened risk for businesses sourcing products and services from overseas.

Snapshot

- Boards must consider the potential impact of various global risks on their physical assets, supply chains, transport and logistics.
- Natural catastrophes and adverse weather remains a major contributor to supply chain interruptions.
- As supply chains have become longer and more complex, so the opportunity for failure at any critical point is greater than ever.
- Companies have a diminished appetite for risk, but tend to lack the detailed information they need to assess supply chain risks.
- By building resilience they can limit downside risks and capitalise on opportunities.
- Resilience involves both business continuity planning and physical loss prevention. Insurance cover is key, as it will fund the mitigation post-event.

> "Companies have invested large amounts of money into trying to improve their understanding of supply chain risk"

To make matters worse, this is all happening in the aftermath of the global financial crisis, at a time when many companies have diminished pain thresholds and/or appetites to assume risk. As a result, unexpected events can have a far greater impact on their business today than before the global financial crisis of 2008.

To date, much of the work undertaken by companies in addressing supply chain risk has been to improve understanding of their supply and value chains. Detailed information is generally lacking in these areas, in part because traditional insurance policies often only pay out in the event of property damage suffered by first-tier suppliers, and therefore do not require risk managers to provide details of suppliers further down the chain.

Becoming conscious of the fact there are third party stakeholders and third party incidents that can impact on a firm's ability to trade is one thing, but being able to pinpoint what those risks might be and address them, and/or plan workarounds in the event of them occurring, is considerably more difficult. This is where the role of the board member responsible for risk, the risk committee or the chief risk officer (see Chapter 1), is vital in bringing together the necessary business functions – procurement, business continuity, finance and operations – to establish a strategic plan that not only ensures business resilience in the event of an incident, but also proactively instils it throughout the organisation.

Building resilience

The benefits of demonstrable resilience are plentiful. It has the potential to make a company a far more attractive investment proposition to shareholders and investors, because of the assumption that future volatility in performance will reduce. Today, the importance of being able to demonstrate resilience is more profound than ever, so it can even become a pillar upon which a company can build its value proposition. In addition, capital invested in identifying business continuity risk allows management to make the best-advised investments in protecting their business, be it through increased physical security, better management systems and programmes, contingency plans, or risk financing/insurance.

Resilience goes further than the typical approach to business continuity planning, and requires taking a broader view where there is fluidity around key processes and assets. It involves understanding that the risk profile around the most critical production streams moves all the time, and that the response of the business has to be more than just a business recovery response. Resilience involves ensuring that some of the business's intangible assets, like reputation, are protected, and is as much about understanding the risk profile as the key business processes. It should focus on the immediate response and behaviour of senior management, just as much as sourcing suppliers and production facilities. Being nimble, with the ability to react quickly to any interruption, can be more useful than a business continuity plan. But flexibility comes from in-depth knowledge of the organisation's operations and the interraction with others. It is about knowing your risks and your options.

All this requires developing an iterative process that recognises that as any one component of the supply chain changes, or if the risk profiles of some critical suppliers change, so the threat potentially changes too. Once it has been established which threats exist, and where the critical points of failure might sit, the difficulty then involves keeping an up-to-date view on suppliers as business continues. Preparation is key and, as natural catastrophe remains one of the biggest risks faced, firms should consider natural hazard zones when deciding on locations and suppliers, and identify the accumulations of risk. Some organisations have significantly improved their understanding by building risk weighting or risk evaluation into their core sourcing and supply chain management protocols, the data for which is generated from a series of self-assessment audit forms to suppliers, and checks on the quality of their controls.

Quantifying exposure

Once identified, supply chain exposures need to be quantified in terms of the financial impact arising from defined risks. This relies on having an informed, detailed understanding of how the business generates revenue and how much of that is exposed, and the key suppliers, processes, people and physical assets that underpin this. Detailed maximum and normal (mitigated) loss estimates can then be calculated, and these are essential to help convince the board that the level of risk requires investment, either by building in redundancy, improving risk management, and/or transfer. The contrast provides a way to place a value on business continuity efforts. Also, as insurers place greater scrutiny on clients' quality and level of supply chain data to safeguard against high loss ratios and aggregated risk, in-depth quantifiable data will go a long way towards securing the limits required at a reasonable price.

Contingent business interruption

There is often an assumption that traditional property damage/business interruption policies will cover a company's supply chain risk. In fact, this is not always the case.

Contingent business interruption (CBI), the interruption to business caused by an incident at an external site (supplier or customer) is covered under the supplier's/customer's extension clause. But beware, this is often direct (first-tier) suppliers only, has a lower limit, and is limted to damage-related events.

A supply chain market has been established to cover an organisation's full supply chain for both damage and non-damage events.

J. HELGASON / SHUTTERSTOCK.COM

Volcanic ash from Iceland's Eyjafjallajökull disrupted air travel in Europe for several weeks

Japan's 2011 Thoku earthquake and resulting tsunami caused major disruption to many global manufacturers' supply chains

The limitations of traditional business interruption and contingent business interruption cover are well documented. Work is being done within the insurance market to develop existing, and promote new, business interruption products to provide cover for disruption to suppliers and service providers resulting from incidents that are unrelated to property damage, such as a pandemic or strike. However, many insured businesses often lack the data on contingent risks and information on second and third-tier suppliers, making the decision of whether such insurance is value for money or not a difficult one.

Beyond insurance

Cover or no cover, building resilience is key in today's just-in-time global supply chain. The businesses that are best able to do this will be those capable of generating the greatest quality of risk management information to help understand where critical points of failure sit, allowing informed decisions on the risks they are prepared to take, as well as those they know they must face.

> “Cover or no cover, building resilience is key in today's just-in-time global supply chain”

Checklist for the board

- **Identify:** Bring together the various business functions – procurement, business continuity, finance and operations – to identify exposures and map the full value chain from remote suppliers through to the final customers.
- **Improve:** Seek to mitigate existing exposures by improving business continuity plans, and those of suppliers. Find alternative suppliers that can be used in the event of an incident, and establish an iterative strategic plan to proactively instil resilience throughout the organisation.
- **Measure:** Quantify supply chain exposures in terms of the financial impact arising from defined risks. Calculate maximum and normal loss estimates, and evaluate any non-financial impacts.
- **Treat:** Use in-depth quantifiable data to secure investment from the board to mitigate supply chain risk, and/or secure appropriate levels of insurance at a reasonable price. How would you know if this is value for money if you have not quantified your exposures?

Chapter 5

Social strains

People-related risks, such as unemployment, social unrest, political instability and income disparity, rank highly among the global risks that threaten businesses today.

John Scott

Chief Risk Officer, Zurich Global Corporate at Zurich Insurance group

Social risks rank highly among the global risks that can impact businesses today. WEF's *Global Risks 2014* report cites risks such as unemployment and underemployment, social and political instability, and income disparity, which all have strong interdependencies as well as links with some underlying global macroeconomic risks.

As Chapter 3 highlights, the global fiscal crisis, triggered by the banking failures of 2008, has had a major knock-on impact on governments' indebtedness, as financial risk has been transferred from private to public balance sheets. The response of governments, especially in indebted, developed economies has driven either austerity budgets and/or ultra-loose monetary policies. These in turn have not only had macroeconomic impacts, such as altered patterns of foreign direct investment affecting emerging economies, but also societal impacts for many countries. All this has taken place against a backdrop of shifting demographic patterns that bring varying challenges to employers around the world.

Snapshot

- The WEF's *Global Risks 2014* report cites several serious social risks to businesses, many of which are interconnected.
- Challenges range from youth unemployment in Western Europe to civil wars in the Middle East and skills gaps in some emerging economies.
- It is important for businesses to understand the issues and take a multi-faceted approach to employment and human resource practices.
- Tackled imaginatively, social risks can throw up opportunities for principled, informed and agile companies.

> "Even the 'stable' Western democracies of Europe have experienced severe civil unrest"

Youth unemployment

The indebted nations of Western Europe and, in particular, in the peripheral countries of the Eurozone, face an enormous challenge in youth unemployment. This presents practical problems for companies in attracting, training and retaining high-quality staff. Those that cease to employ new staff in order to control costs in difficult economic times often find themselves at a competitive disadvantage when the economy recovers. A recruitment gap can mean a lack of succession and a lack of crucial frontline supervisors, who are often key to success in delivering in the marketplace, constraining the ability of businesses to build the capacity necessary to grow.

Young people, even if university-educated, often don't have the specific professional and technical skills required to be successful in the jobs market. Couple this with statistics that say people without full-time employment for more than 10 years are unlikely ever to have a full-time job and the scale of the problem for governments and businesses becomes clear.

Individual companies can go a long way to addressing these problems by putting more emphasis on professional and vocational education and training. Apprenticeships can be invaluable in introducing young people to the workforce and equipping them with the skills to be successful. It seems clear that governments and businesses need to work together to create the optimal mix of professional and vocational training opportunities to drive economic recovery and employment. The private sector can influence education curriculums, guiding them in terms of businesses' requirements and linking them to skills needs. In addition, businesses can work with the education sector to improve apprenticeship opportunities.

As governments respond to fiscal crises with 'austerity budgets' and reduced welfare spending, the onus for providing employee benefits also shifts from the public to the private sector. Innovative approaches to income protection, rehabilitation back into the workplace, employee benefit schemes and employee wellbeing are all being explored as ways to provide support for employees.

Political and civil unrest

The challenges for business of high youth unemployment are even more stark in areas such as the Maghreb region of North Africa, the Levantine and Middle East. A large, well-educated, but underemployed youth population, constrained in entrepreneurial activities by the vested interests of an established elite, can be a powder keg of social and political unrest. This can move rapidly from low-level protest, to outright civil war and regime change, as we have witnessed in several states in the region over the last few years.

Such outcomes are not confined to the Middle East. Even the 'stable' Western democracies of Europe have experienced severe civil unrest and political turmoil related to austerity budgets and high levels of youth unemployment. In these environments, businesses need to develop crisis management to deal with strikes, riots and disruption. All of these can also be triggers for supply chain interruptions (see Chapter 4), for which businesses also need to develop business continuity plans, including arranging substitute suppliers and reserving alternative manufacturing or retail sites.

For some businesses, social and political risks, with their potential for upheaval, can offer new business opportunities, and this shifting political and social landscape should be factored into businesses' scenario and strategic planning activities.

Skills gaps

The picture changes again in the emerging economies, with different drivers of global societal risks. Demographic shifts in North Asia (China, South Korea and Japan) are similar to those in Western Europe and North America with an ageing population. In other Latin American, African and East Asian economies there are large young populations, but the challenge here is often about finding economic opportunities to absorb this workforce. Even though many young people in these regions are becoming better educated, the challenge is about matching the broad-based skill sets required for well-diversified and sustainable economies. In addition urbanisation and migration trends affect businesses operating in these emerging economies. Skills match gaps are particularly difficult to resolve in Africa and the Middle East, while in India and other countries there is a brain-drain of top talent to other regions. The rapidly increasing numbers of people defined as middle-class in terms of their education and purchasing power also creates opportunities for businesses, not only in new consumers, but also as employees who bring a fresh diversity of cultures, talents and interests. The new middle-class in Asia is adaptable and versatile, with access to smart technology and social media. Businesses that exploit and develop this 'digital native' generation will reap competitive advantage far beyond these local markets.

A principled approach

All of this requires companies to have a multi-faceted approach to employing people in the emerging economies. Human resource policies that reflect local requirements and which also support a mobile global workforce become even more important. Portability of employee benefits for globally mobile workers such as pensions and healthcare from one jurisdiction to another, often with different laws and regulations, is just one challenge. Different attitudes across emerging economies to the principles held in the United Nations Global Compact around labour standards, human rights and anti-bribery and corruption policies are also tough 'people challenges' (see opposite).

For a business operating in emerging economies with low-cost manufacturing, even through distant and disparate parts of its supply chain, it is important from a reputation risk perspective – as well as a moral perspective – to ensure that all forms of forced and compulsory labour and child labour are avoided. This can present tough practical challenges, as in some communities removing child workers can exacerbate poverty and result in destitution. Instead, successful companies have found a much better alternative, devising and implementing education and training schemes for young people, providing them with life skills and preparing them for work when they are older.

Opportunity knocks?

The 'Generation Lost?' risk in focus section of the WEF's *Global Risks 2014* report should not be viewed by business as entirely negative. Admittedly, societal risks and trends create tremendous challenges for both governments and businesses to solve. But tackled imaginatively, these risks can also be opportunities for businesses to create a workforce for the future that is both resilient and resourceful – as well as a critical source of competitive advantage.

Doing well, doing good

The UN Global Compact focuses on some key human rights issues, in particular highlighting the problems of child labour and forced labour. These become important considerations for any company with a supply chain that extends into low-cost manufacturing economies.

Next plc is a good example of a company that addresses these concerns in its management of ethical trading. The clothing retailer's approach is to use its influence to promote good practice and raise awareness among both suppliers and employees, as well as others along its value chain. The ethical standards within Next's code of practice apply to all suppliers of its products, in every country where it sources production.

Next's code has 10 key principles, which set out the minimum standards and requirements for suppliers in relation to workers' rights and working conditions, including working hours, minimum age of employment, health, safety, welfare and environmental impacts. The company is very committed, with a dedicated global team that audits suppliers' factories for code compliance, monitors local working conditions and promotes improvements through partnership and support.

Next continues to be an active member of the Ethical Trading Initiative, an alliance of companies, non-governmental organisations and trade unions, striving to ensure the working conditions and rights of workers producing for the UK market meet or exceed international labour standards. The company also supports initiatives and work programmes across a range of supply chains in key sourcing countries.

United Nations Global Contract Principles

Human rights

Principle 1: Businesses should support and respect the protection of internationally proclaimed human rights.

Principle 2: Businesses should ensure they are not complicit in human rights abuses.

Labour

Principle 3: Businesses should uphold the freedom of association and the effective recognition of the right to collective bargaining.

Principle 4: Businesses should uphold the elimination of all forms of forced and compulsory labour.

Principle 5: Businesses should uphold the effective abolition of child labour.

Principle 6: Businesses should uphold the elimination of discrimination in respect of employment and occupation.

Environment

Principle 7: Businesses should support a precautionary approach to environmental challenges.

Principle 8: Businesses should undertake initiatives to promote greater environmental responsibility.

Principle 9: Businesses should encourage the development and diffusion of environmentally friendly technologies.

Anti-corruption

Principle 10: Businesses should work against corruption in all its forms, including extortion and bribery.

Source: UN Global Compact

> “Businesses can create a workforce for the future that is both resilient and resourceful – as well as a critical source of competitive advantage”

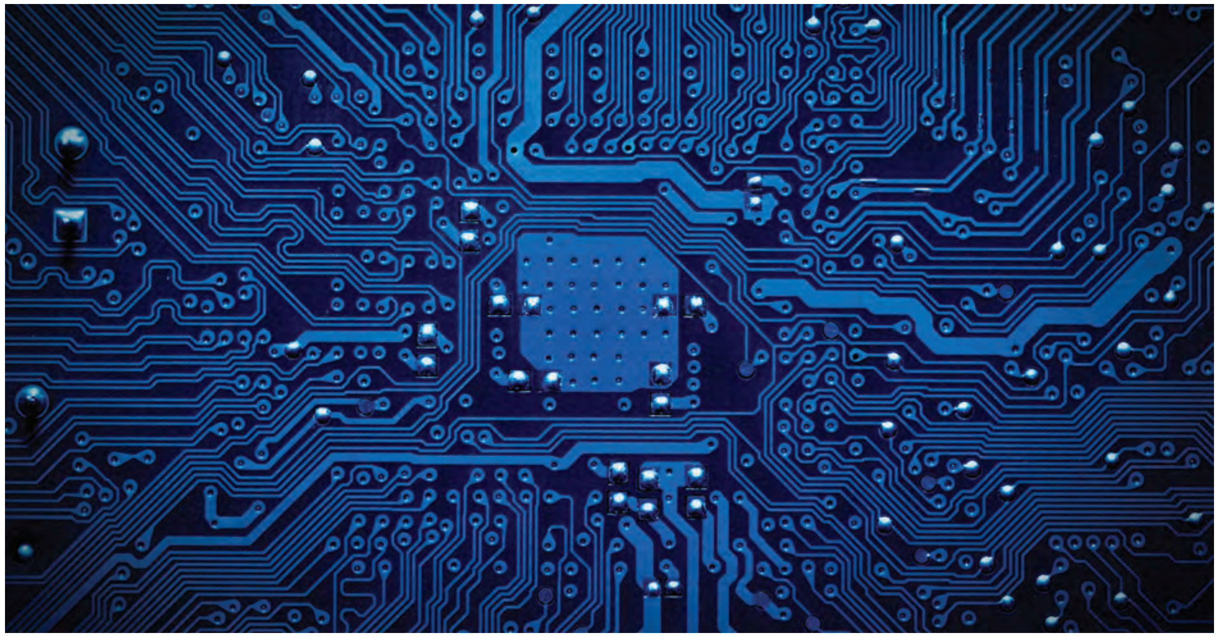
Checklist for the board

- Have we identified how various global social and political challenges could impact upon our business?
- How is our strategy informed by the risks and opportunities these issues present?
- Do we have principles and standards in place, for example on ethical trading, to guide our strategy and operations, and protect our reputation?
- Do we have sufficiently versatile HR policies to manage and mitigate human resource-related risks – and capitalise on opportunities to create competitive advantage?

Chapter 6

Tech traumas

As information technology becomes ever more pervasive, so the opportunities and threats it brings also increase. Boards must respond to these twin challenges.



Charles Beresford-Davies

Managing Director and UK Risk Management Practice Leader, Marsh

It is little surprise that cyber risk featured prominently yet again in WEF's *Global Risks 2014* report, as senior management continues to gain greater understanding of the extent of the cyber threat in today's rapidly changing technological environment. As technology becomes ever more pervasive both at home and in the workplace, many companies have moved swiftly to take advantage of the opportunities that advances have brought. But far fewer have kept up with the risks to their business that such advances have introduced and the financial impact should a vulnerability be exploited.

Cyber attacks regularly make their way into the news, but the incidents described in the media are just a snapshot of what is going on. For example, the UK government has revealed that, on average, 33,000 malicious emails a month are blocked at the gateway to its secure intranet. The volume of e-crime and attacks on industry is equally disturbing. Attempts are made to steal British intellectual property in a wide range of industries, not just in defence and security. Globally, cybercrime is estimated to cost the world economy $500bn[1] a year.

For those companies that fall victim to this new breed of cybercriminal, 'hacktivist', and/or cyber terrorist, the operational disruption can be huge. There is also the internal cyber threat from negligent employees and contractors, which – at a time when concerns surrounding privacy and data protection are more prominent than ever – can have disastrous reputational, and ultimately financial, consequences.

THREAT ENVIRONMENT

Criminal

- Personal information
- Credit/debit card information
- Held funds
- Intellectual property

Terrorist or State

- Disruption to critical infrastructure
- Economic impact
- Loss of life
- Damage to property

Malice

- Disgruntled employee/customer
- Proof of ability
- Untargeted malicious code
- Random selection

'Hacktivist'

- Public support for a cause
- Direct impact of core activity
- Corporate or industry-wide scandal
- Top corporate brand target
- Disgruntled employee/customer
- Proof of ability
- Untargeted malicious code
- Random selection

Internal

- Loss of hardware
- Data mismanagement
- Negligence

Yet where there is risk there is also opportunity. In today's fast-paced, just-in-time business environment, trust and reliability are revered by clients and business partners alike, and just as there is huge downside risk for those companies that fail to demonstrate these characteristics, there is also vast potential for competitive advantage for those that succeed in establishing themselves as a paragon of security and dependability.

Our reliance on technology is growing and the pace of technological change is increasing. Today, for example, there are 14.4 billion devices connected to the internet, and by 2020 it is predicted this figure will surpass 50 billion.

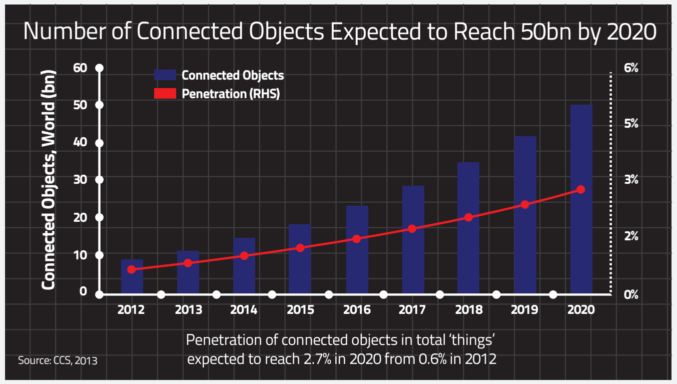
The opportunities this growth presents for businesses are huge, but so too are the risks to their operations and security. This increase in online devices will result in much greater and much more complex interconnectedness between people and their devices – and therefore between devices in general – as well as a three-fold increase in the number of potential entry points for those bent on disruption.

At a time when so many components of a business's day-to-day operations are technologically-dependent, companies cannot afford to treat IT security as a peripheral risk that can be outsourced to third-party security providers, or even left to the responsibility of the chief information security officer (CISO).

Snapshot

- The internet is a powerful engine for growth, commerce and social development. It will continue to offer huge opportunities.
- But technological threats cast a shadow over all organisations, regardless of size or location.
- Incidents described in the media are just a snapshot of a disturbing volume of cyber crime and electronic attacks on industry.
- Basic information risk management can stop the majority of cyber attacks seen today, but experience suggests that few organisations get it right.
- Information security and cyber security are issues that all boards need to own directly.

> “In today's just-in-time environment, trust and reliability are revered by clients and business partners alike”


Number of Connected Objects Expected to Reach 50bn by 2020

Penetration of connected objects in total 'things' expected to reach 2.7% in 2020 from 0.6% in 2012

Source: CCS, 2013

Instead, it requires a holistic board-led strategy that nurtures awareness and expertise with regard to technological dependencies and liabilities throughout the organisation.

The starting point for this is the board itself. At a time when business performance is so closely aligned with companies' ability to use technology effectively, only 16% of board members have previous experience working as a CISO or senior IT executive[2]. Boards across the world have traditionally been filled with people with expertise in a variety of disciplines, and it is now more important than ever that they bring in more members with the technological nous to guide their companies around cyber issues.

The nature of a business's approach to cyber risk is essential too. Technological innovation is now moving at such a pace that an IT security policy comprising antivirus software and a few firewalls is simply insufficient. Instead, companies must maintain a dynamic and nimble position from which they can rise and adapt to the cyber challenge, as opposed to taking up a defensive stance in the hope of repelling the incoming threat. Defence alone is not nearly enough. Instead, an approach is required that detects opportunities resulting from technological innovation, while identifying and mitigating accompanying cyber exposures, as well as those of legacy systems. In this respect, responsibility for cyber security needs to sit above the role of CISO. It must sit with the board, because it is the board that, while not managing day-to-day cyber risk responses, needs to be satisfied that they are robust.

Top-down work must then be carried out to map all areas of a company's technological infrastructure, data-related tools, and systems and processes. This will make it much easier to establish those points of weakness that are traditionally found at connection points between programmes and systems. With these areas identified, businesses can begin to quantify the risk in terms of its potential financial impact, and develop an incident response plan in case an incident should ever occur. This should involve undertaking a programme to improve the general understanding of the company's technological structures, and how they are integrated, throughout the entire organisation.

Implementing strict standards and policies to ensure every employee knows how to work with the company's technological infrastructure is essential, both to ward off the external cyber threat and to limit the potential for internal negligence to result in the loss of data and/or network control. It is important to accompany such a cyber policy with a means of control whereby senior management can guarantee that standards are being adhered to, not least to avert the potential reputational and regulatory consequences of mismanagement.

Boards own cyber risk

A key role for the board is to consider the organisation's cyber risk appetite, not least in terms of trade-offs between the security of information systems and their usability.

It is important for the board to understand what levels of risk can be accepted in any business model that relies on information systems and the internet for delivery.

Considerations that go far beyond the technical issues should be included in this decision. For example, what efforts have been put in place to vet the security of employees in critical data-sensitive roles – also bearing in mind that these roles are often outsourced? Bribery and blackmail are as effective as sophisticated phishing attacks or malware at getting employees to reveal sensitive passwords.

Physical security and information security become intertwined topics that any cyber security policy needs to take into account. The board should not allow this issue to become solely the domain of technical experts. It is as much about employee vetting and clean desk policies as it is about patch management and malware detection.

Insurance can also play an important part in a business's cyber mitigation strategy. While the development of cyber cover is still in its early years, products are evolving rapidly as insurers learn more about what their clients need, and the risks that they themselves are willing and able to accept. Present policies are predominantly focused on protection against privacy breaches and data theft. Typically, this has been a response to legislation, in the US in particular. In Europe and elsewhere businesses are increasingly seeking broader protection for a wider range of impacts, most notably business interruption arising from critical systems failure. The insurance industry is listening to business concerns, and we can expect developments to be made in new technological risk areas in future.

With or without insurance, cyber risk can never be truly eliminated. Those companies that adapt best to their technological surroundings – exploiting the opportunities as well as managing the risks – will be those best placed to survive and thrive. Ultimately, however, cyber risk is a global issue, and a much greater degree of information sharing between governments and businesses worldwide should be encouraged to improve awareness of existing and emerging threats. Recent high-profile revelations about the activities of national security organisations may have set back progress on this front, but it is difficult to envisage how the balance of advantage can be tipped from attackers in favour of defenders without concerted, cross-border business and governmental collaboration.

> “While the development of cyber cover is still in its early years, products are evolving rapidly as insurers learn what their clients need”

[1] *The Economic Impact of Cybercrime and Cyber Espionage*, McAfee and the Center for Strategic and International Studies.
[2] *Taming Information Technology Risk: A New Framework for Boards of Directors*, Oliver Wyman and the National Association of Corporate Directors.

Checklist for the board

- Implement a board-led, holistic approach to cyber risk and opportunity, and ensure there are board members in place with the technical expertise to help drive this.
- Maintain a dynamic and nimble stance on cyber issues, which can continuously be adapted to the rapidly changing risks.
- Develop a cyber risk appetite based on the trade-offs between security and system usability.
- Map all areas of technological infrastructure, data-related tools, systems and processes. Link physical data and security policies with your new cyber-risk approach.
- Quantify the risk in terms of its potential financial impact, and develop an incident response plan in case an incident should ever occur.
- Improve the understanding of technological systems and how they are integrated, and implement a means to guarantee that best practice information and physical security standards are adhered to.

Chapter 7

Reputational ruin

Global risks can cause damage to a company's reputation, with significant revenue loss and the destruction of stakeholder trust. But boards can manage the risk and create opportunities

Faye Whitmarsh
Senior Manager,
Culture and Behaviours,
PricewaterhouseCoopers

Richard Sykes
Partner and Head of
Governance, Risk &
Compliance, PwC

While the risks contained in the WEF's *Global Risks 2014* report can be managed individually, boards should consider their wider potential effect on a firm's reputation. The reputational aspects of managing risk can be the defining factor in determining business winners and losers. They rightly receive prominence in the both the latest WEF report and Airmic's 2014 study *Roads to Resilience* (see page 34).

Damage to an organisation's reputation can result in significant revenue loss and the destruction of stakeholder trust. Today, with social media adding a new dimension, it can happen in an instant. Depending on how it is managed, social media can add a further substantial threat to an organisation's reputation, or it can present new opportunities.

Reputational risk links to trust

The foundation of an organisation's reputation is the trust of its stakeholders. This is built on the organisation's ability to deliver on its promises to customers, employees, investors, regulators and the media. Ultimately, an organisation is the sum of its people – and their actions.

Your people may be your most important asset, but they can also represent a hidden business risk. And not just through isolated fraud, data security or privacy breaches. People do not tend to act on the spur of the moment or in isolation. Their behaviour is likely to have been influenced by the culture of the organisation over time. It is paramount, therefore, to consider behaviours and the culture of the company as a fundamental component of building a resilient organisation and managing emerging business risks. It is a lot more than just managing systems, processes and procedures.

In order to best demonstrate its ability to deliver on the promises it makes, aligning an organisation's purpose, vision and values to the actual behaviours demonstrated by its leaders and employees is critical.

If there is a mismatch between what you say and what you do, you risk losing trust. This can be damaging to motivation, performance and reputation.

Aligning purpose, vision and values

To ensure that an organisation is engendering a strong culture that is aligned to its values and business objectives, it is important to examine why it exists. What are the purpose, vision and values of your organisation? What behaviours do you need in place to deliver them? Do your policies, processes and procedures drive the required behaviours?

Aligning your intended, espoused and actual behaviours is the key to demonstrating your ability to deliver on your purpose, vision and value and delivering on your promises.

Your purpose, vision and values need to be protected, embedded, monitored and discussed on an ongoing basis at all levels of the organisation. These ultimately drive the right decisions for your reputation, ensuring your actions reflect what you stand for as an organisation.

Snapshot

- Boards should consider the potential effect of the impact of global risks on their company's reputation.
- Managing and mitigating these impacts begins by building trust.
- Organisations must strive to align their purpose, vision and values to the actual behaviours demonstrated by leaders and employees.
- Opportunities, as well as resilience, will emerge from building the right corporate culture.

> "Your purpose, vision and values need to be protected, embedded, monitored and discussed at all levels"

ALAMY

Firms profiting from sweatshop labour risk public shame

Principles, not rules

Promoting empowerment can help build an organisational culture that enables your business to be more agile. This allows for faster decision making. Getting employees to think within an ethical framework, rather than blindly following rules, engenders trust and allows for faster, better decisions that align to your purpose, vision and values. This is particularly helpful when you consider that most business decisions require a trade-off: for example, what takes priority – customer or profit? Making the right decision at key moments is critical to delivering on your promises and remaining aligned to your values.

Tension can exist between the control that organisations seek and allowing people freedom to make decisions and be responsible for them. Finding the right balance can be a challenge. It will not be achieved by acting like 'Big Brother', but by discovering how your organisation can enable and encourage the desired behaviours whilst disabling and discouraging the undesirable.

Practical steps

Within the most successful organisations, culture and behaviours are seen as a board-level issue of strategic importance. Behavioural expectations need to be clear. People at all levels are personally accountable and know what is expected of them. The tone from the middle and tail are taken into account alongside the tone from the top. Successful organisations recognise that leadership can operate at all levels. Alignment is essential, so critical behaviours are clearly defined and aligned to purpose, vision and values and, crucially, measured. If behaviours are strong and aligned this can help enable the achievement of business objectives, which can be the best control for your business.

An organisation's purpose, vision and values reflect the society within which it operates. Our social values change over time: some things that were acceptable 50 years ago are not today, for example, wasteful packaging or smoking in the office. Applying a 'yesterday, today and tomorrow' lens to your decision-making can ensure that you stay aligned to your, and society's, values. It will help the board to deliver against the objective of driving decision-making that is ethical and aligned to social values.

When reflecting on decisions your organisation has made in the past, hold these up to today's values – this is where any 'skeletons' may emerge from the past that need to be dealt with. When making decisions for today, make sure they are aligned to today's purpose, vision and values and uphold what you stand for as an organisation. Considering likely future decisions can often be the most challenging. While we do not know what society will value in the future, there are significant clues in the WEF's *Global Risks 2014* report as to what developments may occur. In particular, WEF highlights the societal trends of longevity, income disparity, unemployment and underemployment. In the meantime, you can feel secure in decisions and actions that support current societal values. Should those need to shift in the future, you can take steps to modify your actions over time.

Opportunities, as well as resilience, emerge from building the right corporate culture. For example, you are more likely to attract and retain talented people and, by enabling a more collaborative culture, you may encourage greater innovation. Advocating a culture of 'speak up and challenge' will also enable problems to be highlighted, escalated where necessary, and resolved efficiently.

Culture change

We are starting to see organisations in the banking sector develop comprehensive cultural assessment and measurement approaches to enable them to effectively monitor their behaviours.

One of these organisations had recently conducted a major behavioural change programme as the result of an unauthorised trading incident. By undertaking a detailed review of the design and operational effectiveness of this programme it was able to provide comfort to management and the industry regulator that the required change in behaviours was occurring. This included testing key controls to ensure that the right people were being recruited, promoted and trained, and that consistent values and underpinning behaviours were embedded across the business.

Increasingly, organisations are measuring their culture and behaviours to discover where to focus interventions and to ensure they are achieving the desired cultural state.

GETTY

Word spreads: Northern Rock's customers rapidly withdraw their savings on news of the bank's crisis

A question of ethics

The Institute of Business Ethics (IBE) recently published its triennial survey of the mechanisms used by large companies to embed ethical values within business practice and provide guidance to staff. One of the most notable findings of the study is the evidence of increased investment into ethics programmes, with 70% of UK and European businesses polled saying they have increased such investment over the last three years, compared with 50% saying this in 2010. Furthermore, 87% of UK respondents state that a board member takes ultimate responsibility for the ethics programme, suggesting that the embedding of ethical values is being given a high priority at board level.

However, ethics is only a regular board agenda item for 65% of UK and 70% of other European companies. "When you consider the cost of ethical failures to a company's reputation, it is a cause for concern that more boards are not regularly assessing their company's ethical performance," says the IBE.

> “Applying a 'yesterday, today and tomorrow' lens to decision-making can ensure that you stay aligned to your, and society's, values”

Checklist for the board

- Have we recognised the potential for global risks to impact upon our reputation?
- Are our purpose, vision and values aligned to our actual behaviours?
- Is this alignment regarded as a strategic issue for the board?
- What practical steps can we take to create the right organisational culture?

Chapter 8

Creating resilience

As well as taking measures to manage and mitigate short-term disruptions, businesses should strive to create a framework that will support longer-term enterprise resilience

James Crask
Senior Manager, Business Resilience, PricewaterhouseCoopers

Richard Sykes
Partner and Head of Governance, Risk & Compliance, PwC

We often focus on managing the downside of risks at the expense of the opportunities presented by them. This guide has sought to address this issue by setting out how organisations can balance negative risk impacts against the opportunities arising out of expected and unexpected change. This chapter goes further. Existing organisational structures, which protect against short-term disruptions and change, need to be supplemented with a framework that will support enterprise resilience over the long term.

The need for a focus on enterprise resilience stems from three issues:

1. Traditional enterprise risk management is not enough. It has difficulty in capturing how to respond to events that are truly unique and unknown. And it is unsuited to managing the consequences of every decision taken by an organisation.

Snapshot

- Boards should consider opportunities as well as downside risks, and longer-term resilience as well as short-term business continuity.
- Businesses should take a broad approach, incorporating their sustainability principles, to maximising resilience across all areas of activity, from product or service design, to supply chain flexibility.
- True enterprise resilience requires an organisation to anticipate and adapt to change in order not only to survive, but to evolve.
- Enterprise resilience is dependent on strong leadership.

> “An enterprise resilience framework will help to actively manage both the downside and upside from risk”

2. Companies still fail, or suffer major disruptions, despite heavy investment in a range of risk management activities, suggesting there are other factors required to support resilience.

3 The relentless pressure on businesses to cut costs while enhancing their long-term prospects of survival means that agility can sometimes be at odds with the requirement for robust protection mechanisms. For many, this can result in poorly considered investments in resilience. The ‘buffers’ that contribute to resilience are increasingly seen as an unnecessary expense and are removed to reduce costs.

There is a requirement to think more broadly about how to enhance the long-term sustainability of an organisation against a backdrop of constant change. Existing risk management activities need to be supplemented with a broader focus on a series of interrelated factors that contribute towards resilience. There will always be uncertainty, but a uniform and integrated model against which to measure an organisation’s resilience can provide an invaluable source of intelligence to support decision making.

Crucially, resilience is a quality rather than an absolute. No organisation can say it is completely resilient, making it hard for it to visualise what delivering enhanced resilience might look like. For many, their response to this issue has been to ‘de-scope’ their approach, focusing on the more tangible and readily understood aspects of risk management at the expense of the broader factors that drive enhanced resilience.

Businesses will always need the ability to identify and manage risk, and to deal with sudden shocks, disruptions and crises. As most leaders are aware, however, this is not enough to create true enterprise resilience, which is a state that is enhanced or diminished by an organisation’s ability to anticipate and react to change in order not only to survive, but to evolve. This is reinforced by a recent report by Airmic and Cranfield School of Management, *Roads to Resilience*, which found that resilience is created or reduced by much more than an organisation’s ability to manage risk (see page 34).

Leveraged in the right way, an enterprise resilience framework will help organisations actively manage both the downside and also the upside from risk, as well as changing, and freeing-up precious resource from, the near constant focus on individual risks.

The model for enterprise resilience

Resilience is much more than the sum of the risk management parts that protect the organisation from harm. It can be created or depleted by everyday decisions, behaviours and activities as well as corporate strategies.

Resilience can be enhanced or eroded in four dimensions:

- The ever-changing personality of an organisation, its culture, values, purpose and mission

- The degree to which an organisation's networks, interdependencies, context, environment and likely futures are truly understood
- The activities undertaken, including those to protect the organisation from harm
- By an organisation's rules, behaviours, norms, innovations and leadership.

The operational aspects of resilience, including risk management, business continuity, IT resilience, crisis management and information security management, to name a few, are never likely to be less important than they are today, and in fact need to exhibit a much higher degree of collaboration in delivery. Organisations that focus excessively on these areas at the expense of the wider factors that contribute towards resilience could perversely be diminishing their overall levels of resilience. A mature business will generally mix these activities, which aim to address shorter-term risks and impacts, with a consideration of a wider range of resilience factors that draws on the characteristics that define the business and can guide its decision-making. Few businesses, however, have identified these wider elements clearly and consistently in every department and at every level. To give an example, creating a code of values is useless if only half the workforce identifies with it.

Leadership for resilience

Leadership plays a crucial role in building resilience. Leaders committed to creating more resilient organisations typically demonstrate authenticity, build trust that enhances social capital, maintain an awareness of an organisation's current and future relevance, and innovate accordingly. These leaders have in-depth understanding of their organisation and the networks and circumstances upon which they rely. Their deep understanding is embedded within both everyday and strategic decision-making. They also empower staff to take ownership of decisions, including delegating risk management tasks along with the ability to raise issues, ideas and innovations that will help the organisation to manage change positively.

When great leaders talk of making their organisations more resilient, they speak from a position of understanding their business and the context in which it operates.

Leaders focus on:

- The capability to respond when needed
- Placing sustainability at the centre of their strategy and decision-making framework
- The agility to move quickly and decisively when required.

In delivering resilience, leaders are concerned about:

- Shared values
- Disciplined innovation

Roads to Resilience

Roads to Resilience, a 2014 report published by Airmic, highlights that effective risk management goes way beyond compliance or adherence to standards. The findings have profound implications for both boards and risk professionals.

Roads to Resilience follows up on *Roads to Ruin*, also from Airmic, which looked at high-profile crises involving 23 companies that left their reputations in tatters. The latest report demonstrates, through a series of in-depth case studies, that successful corporate resilience is not characterised by an absence of the key points of failure outlined in *Roads to Ruin*. In resilient organisations, risk management was found to be integrated into strategic and operational decision-making and formed part of the very essence of the corporate identity.

Airmic and Cranfield School of Management studied leading organisations that have created a resilient culture, protecting their business and reputation. They found the incentive to become resilient goes well beyond avoiding disaster. Firms that are sure of their risk management also have more confidence to be enterprising, not only identifying risks but also seizing opportunities.

The research found that the qualities embedded in resilient organisations enable them to succeed in other respects. They are more responsive to their customers and the markets they serve, their staff and suppliers are motivated and loyal, they gain trust by being more dependable, and achieve better results for shareholders.

In short, resilience should be at the heart of strategy and part of the overall vision of every organisation.

- Genuine social capital with customers, staff, regulators and the public at large
- People who work with and for them and their behaviours
- Intelligently integrated risk management activities that cooperate to protect all key assets and aspects of the organisation
- Having the right skills, competencies and other resources in the right place at the right time.

The importance of measurement

Many of the factors that contribute to an organisation's resilience are harder to visualise than functional or operational processes, but they are not impossible to measure or manage. By gauging the level and impact of the factors that contribute directly to an organisation's level of resilience, leaders are able to make better-informed choices and adjust their strategies to leverage competitive advantage.

The importance of these factors will vary between each organisation depending on a range of dynamic factors, including purpose, environment, context and culture. This means that any approach to measurement must be tailored to these factors.

Survive and thrive

Enterprise resilience is not just about surviving in the present. It is about having the foresight, capability and agility to adapt and evolve; to identify and take advantage of opportunities as well as address challenges; to thrive as well as survive. Enhancing an organisation's resilience cannot be achieved in silos. It requires coordination and action across all locations, within all functions, and at all levels of an organisation.

It remains important for an organisation to consider how it might respond to individual risks, not least those highlighted by the WEF's *Global Risks 2014* report. But investments in managing such risks can be wasted if delivered without considering the integration of the wide range of activities an organisation undertakes to protect its interests. A broad approach is required, with clear focus on the interrelationship between various factors that combine to make an enterprise more resilient.

> “Enterprise resilience is not just about surviving in the present. It is about having the foresight, capability and agility to adapt and evolve”

Checklist for the board

- Are we currently protecting the right parts of the business?
- What are our current levels of resilience across the organisation?
- Are functional silos collaborating and working as effectively as they should?
- Are we spending wisely with our investments in resilience?
- What aspects of resilience are most important to us?

Chapter 9

It could be you...

Some final thoughts and key tasks for the board

John Hurrell
Chief Executive, Airmic

This guide has highlighted that global risks are among the most dangerous an organisation can face. These threats move fast: a pandemic could go global in weeks; the 2007 financial market crisis caused mayhem in days; and political and military events, like the recent turmoil in Ukraine, spur rapid change. Yet global risks also offer opportunities for well-prepared businesses. The very fact that such risks are systemic means they are likely to affect your competitors as well as you, and then the most resilient companies will survive at the expense of the rest.

Airmic's *Roads to Resilience* research shows that one of the critical aspects of resilience is adaptability. This entails having an effective 'risk radar' (boards should subscribe at low-cost to up-to-date sources of intelligence on key political, economic, financial and market trends), excellent communications and empowered management. Here, SMEs hold an advantage over large corporations in their speed of response.

The impact of a global risk is likely to attract significant media attention, putting the reputation of businesses involved on the line. Those seen to be part of the solution – delivering for customers, employees and other stakeholders despite challenges – stand to reap long-term reputational benefits.

Ultimately, company boards cannot anticipate every eventuality and even the best prepared can be blindsided by 'black swan' events. But, as this guide has highlighted, there are many decisive steps that they can, and should, take.

Key tasks for the board

- Seek to understand the nature and extent of global risks, with the help of expert analyses such as *WEF's Global Risks 2014* report.
- Look at your organisation's critical dependencies, including people, physical assets, financial support, supply chains and technology, and assess major areas of vulnerability.
- Adopt a strategic approach and appropriate operational tools to build resilience – from scenario planning and business continuity management to people policies – ensuring that robust measures are in place to manage and mitigate the impact of global risks.
- Demonstrate leadership by: clearly taking board ownership of global risk oversight; adopting a strategic mindset that is open to opportunities as well as wise to threats; observing principles of sound governance and regulatory compliance; implementing appropriate internal structures and policies; and adhering to – and communicating – an ethical and sustainable approach.

Contributors

Tap play buttons for videos

Dr Roger Barker is Director of Corporate Governance and Professional Standards at the IoD. He is Senior Adviser to the Board of the European Confederation of Directors' Associations (ecoDa) and Chairman of its Education Committee. He sits on the advisory board of the Institute of Chartered Accountants in England and Wales and is a visiting lecturer at the Saïd Business School (University of Oxford), ESSEC (Paris), UCL (London) and the Ministry of Defence in the UK.

John Scott is Chief Risk Officer for Zurich Global Corporate, where he leads the implementation of the Group's enterprise risk management strategy. A graduate of Oxford University, with a PhD in Geology, his early career was with BP in the upstream oil and gas industry. In 1995 he gained an MBA at Cranfield and joined BOC, later becoming General Manager of BOC's Edwards business division. He currently chairs the Carbon Capture and Storage Association's (CCSA) group on risk.

James Sproule has been Chief Economist and Director of Policy at the IoD since January 2014. Prior to joining the IoD, he led Accenture's UK Research and Global Capital Markets Research. He started his financial career as a merchant bank economist, working at Bankers Trust, Deutsche Bank and Dresdner Kleinwort, and eventually helped to found the boutique bank Augusta and Company. Before embarking on a career in economics, he was a signals officer in the Royal Navy.

Caroline Woolley is Property Practice Leader at Marsh and responsible for the company's risk practices and its global Business Interruption Centre of Excellence. She was previously in Marsh Risk Consulting's Forensic Accounting and Claims Services team, where she was head of the Forensic Accountants. She has written numerous articles on forensic accounting, business interruption and supply chain-related topics, and also received the *Business Insurance* global 'Women to Watch' award in New York in 2011.

Charles Beresford-Davies is head of the Marsh UK & Ireland Risk Management Practice, Marsh's major account management business. Prior to this appointment in 2012, he led the Marsh UK Financial Services Practice for seven years following his return to Marsh from Jardine Lloyd Thompson in 2005. His 24 years in the insurance business began with Lloyd's of London, but for much of his career he has focused on insurance brokerage within the international financial services sector.

Richard Sykes is a Partner and Head of Governance, Risk & Compliance at PwC, where his current focus is on driving the risk resilience agenda. He has contributed to several thought leadership publications around risk and compliance by PwC, the IoD, Tomorrow's Company and others. He has spent the majority of his career as an audit partner on FTSE 100 clients and he is currently PwC's global relationship partner for advertising group WPP and insurance company Old Mutual.

Faye Whitmarsh leads PwC's Risk Assurance culture and behaviours team, which specialises in assessing and measuring culture and behaviours. This includes conducting cultural assessments, designing behavioural measurement frameworks and assessing the effectiveness of behavioural change programmes. She holds an MSc in Organisational Psychology, adding a psychological lens to her skills in risk assurance and business resilience. Much of her current work is for clients in the financial services industry.

James Crask is Senior Manager in PwC's Enterprise Resilience team, where he advises clients on how to improve their resilience. He regularly coaches and speaks on this theme and has advised the UN International Strategy for Disaster Risk Reduction, exploring the private sector's role in managing disaster risk. He is currently helping to develop a new International Standard for Organisation Resilience. Before joining PwC, he worked for the UK Cabinet Office Civil Contingencies Secretariat.

John Hurrell has been Chief Executive of Airmic since 2008, following a career of almost 30 years in the Marsh and McLennan Group of Companies, where he was Chief Executive of Marsh's Risk Consulting business throughout Europe and the Middle East for five years. At Airmic he has led extensive research into risk and insurance-related issues, resulting in a number of groundbreaking publications, including *Roads to Ruin* (2011) and *Roads to Resilience* (2014).

Responding to global risks

The World Economic Forum's recent report, *Global Risks 2014*, analysed dozens of global risks, based on a survey of over 700 experts from industry, government and academia. This publication builds on the WEF report's findings by describing practical measures that businesses can take to manage and mitigate these risks.

Written by leading experts in the field of business risk management, this guide is particularly aimed at board-level directors, from all industry sectors, including public sector organisations. It offers global perspectives for multinational companies, as well as local implications for smaller firms. It is also relevant to risk professionals and others who wish to understand global risks and the distinctive role of the board in responding to them.

airmic
Together Leading in Risk
www.airmic.com

MARSH

pwc

ZURICH®

IoD
Institute of Directors
116 Pall Mall, London SW1Y 5ED
www.iod.com