

# Enterprise Risk

Spring 2016 / [www.enterpriseriskmag.com](http://www.enterpriseriskmag.com)

The official magazine of the Institute of Risk Management

---

**Bribery conundrum:** when to defer prosecution / **Deadly legacy:** learning from asbestos / **Written in stone?** applying ERM to strategy / **Enhance your influencing:** effective communication / **Into the breach:** dealing with hackers



**The Forever War:** Stuart Sterling on the UK Government's cybersecurity strategy



Aon Risk Solutions

# **DATA** and **ANALYTICS** shaping the **FUTURE** of **RISK**

How will you address  
the top global risks?

*For further information please visit*  
**[aon.com/2015GlobalRisk](http://aon.com/2015GlobalRisk)**

Risk. Reinsurance. Human Resources.

**Aon**  
Empower Results®



Spring 2016

## Editor

Arthur Piper

## Design and Production

Smith de Wint  
Antenna Business Centre  
Beck Street, Nottingham, NG1 1EQ  
Tel: +44 (0)115 958 2024  
risk@sdw.co.uk  
www.sdw.co.uk

## Sponsorship and

## Advertising Sales Manager

Clementina Christopher  
clementina.christopher@theirm.org  
Tel: +44 (0)20 7709 9808 Ext. 234

Enterprise Risk is the official publication of the Institute of Risk Management (IRM).

ISSN 2397-8848

IRM is the leading professional body for enterprise risk management. We are an independent, not-for-profit organisation that champions excellence in managing risk to improve organisational performance.

We do this by providing internationally recognised qualifications and training, publishing research and guidance and setting professional standards across the world. Our members work in all industries, in all risk disciplines and across the public, private and not-for-profit sectors.

## Institute of Risk Management

2nd Floor, Sackville House, 142-149  
Fenchurch Street, London, EC3M 6BV  
Tel: +44 (0)20 7709 9808  
Fax: +44 (0)20 7709 0716  
enquiries@theirm.org  
www.theirm.org

Copyright © 2016 Institute of Risk Management. All rights reserved. Reproduction without written permission is strictly forbidden. The views of outside contributors are not necessarily the views of IRM, its editor or its staff.



# Editorial



## Your magazine gets a makeover

Welcome to your new look magazine. It has been renamed, redesigned and revamped. I hope you like the results as much as we do.

Let me talk you through what we've tried to achieve. First, the name. The IRM rightly believes that while risk management is a broad church, the overriding methodology underpinning best practice is encapsulated through enterprise risk management. Strictly speaking, that could have served as the new title of the publication – but it's too long for the front cover. That's how risk management professional – the magazine's previous name – ended up being the rather vague *RM Professional*.

We canvassed some members and enough of you liked it for us to go ahead and call it *Enterprise Risk*.



While risk management is, of course, a technical subject in many ways, it's also about people and places – something we want to capture in the magazine

Second, the design. We've gone for a contemporary look and feel – with an innovative choice of paper that makes the photography sing out. The paper, to get all technical for a moment, is bonded paper. That means it's not glossy like most trade magazines, but has a warmer look and feel – like art house magazines. It helps give the clearer, more flexible design and fonts an up-to-date feel at the same time as enhancing readability.

Finally, the content. While risk management is, of course, a technical subject in many ways, it's also about people and places. That is something we are keen to capture in the magazine with more profiles, photojournalism and risk managers featured in each issue. As we develop the content, we want to make sure that you can learn from those at the cutting edge of the profession by featuring their work in the magazine.

We'll also be featuring key stakeholders from outside the profession whose work directly impacts your own. In this issue, for example, we speak to Stuart Sterling, who is leading the UK Government's efforts to get private business up to speed in the war on cyber crime. And we'll be provoking thought via regular columns by the IRM's chief executive Ian Livsey and our new end page Toffler.

Please let me know what you think.

Arthur Piper

Editor

# NOW YOU CAN KEEP AN EYE ON YOUR RISKS FROM ONE PLACE.

Protecting the business you love is easier when you have a clear view of what might affect it. My Zurich is an online portal that gives you 24/7 access to real-time claims data, the status of your policies and wordings, including benchmarking for risk engineering data, in a transparent way.

**FIND OUT MORE AT**  
**[zurich.com/my-zurich](http://zurich.com/my-zurich)**



**ZURICH INSURANCE.**  
**FOR THOSE WHO TRULY LOVE THEIR BUSINESS.**



This is intended as a general description of certain types of insurance and services available to qualified customers through subsidiaries within the Zurich Insurance Group, as in the US, Zurich American Insurance Company, 1400 American Lane, Schaumburg, IL 60196, in Canada, Zurich Insurance Company Ltd, 100 King Street West, Suite 5500, PO Box 290, Toronto, ON M5X 1C9, and outside the US and Canada, Zurich Insurance plc, Ballsbridge Park, Dublin 4, Ireland (and its EEA branches), Zurich Insurance Company Ltd, Mythenquai 2, 8002 Zurich, Zurich Australian Insurance Limited, 5 Blue St., North Sydney, NSW 2060 and further entities, as required by local jurisdiction. Certain coverages are not available in all countries or locales. In the US, risk engineering services are provided by The Zurich Services Corporation.



10

## FEATURES

### 10 The Forever war

Stuart Sterling is leading the UK Government's efforts to get the private sector engaged in the war against cyber crime

### 14 Once more into the breach

Cyber attacks can be a nightmare for businesses to prevent, detect and deal with, so why don't organisations put more effort into getting ahead of the game?

### 18 White gold's deadly legacy

Controlling the use of hazardous products in developing countries is hard. Businesses, governments and society need to learn the lessons from the global tragedy that asbestos is still leaving in its wake

### 22 The bribery conundrum

Two recent successful investigations by the SFO have raised questions for risk managers on how and when to report potential bribery misdemeanours to the authorities

### 26 Enhance your influencing

Risk managers need to be able to influence those around them if they are to be effective

### 30 Written in stone

Risk managers should not treat an organisation's strategy as though it were written in stone. Applying enterprise risk management to strategy is key to ensuring its success



14



18

## REGULARS

### 07 CEO's message

If risk managers are going to get to grips with cyber risk they will need to dig beneath the surface

### 08 Trending

Recurring images of makeshift migrant camps have dominated recent news. But coming years will see attention turn to environmental risk

### 35 Institute news

The latest on IRM initiatives, conferences, courses and training

### 36 Directory

In need of insurance services, a range of risk management software and solutions, or training – look no further than our listings

### 38 Toffler

Is the rate of change really accelerating?



22



26



30

# Collaboration

# Team Work

# Ownership

# Symbiant®

a sensible solution

a sensible price

## **The Total Risk, Audit and Compliance Software solution**

Symbiant is a modular solution that allows the whole workforce to collaborate on Risk, Audit and Compliance issues with prices starting at only £200.

Risk Registers, KRI, Incident Management, Dashboards, Action Tracking, Planning, Questionnaires, Control Assessments....



**To find out more or to arrange a free trial visit:**

**[www.symbiant.uk](http://www.symbiant.uk)**

Trusted by names you know from Charities to Banks, Government to PLC.

**Symbiant®**  
Better Software



## A challenge to stay relevant



*Much of what makes technology work is hidden behind glossy interfaces, but if risk managers are going to get to grips with cyber risk they will need to dig beneath the surface*

---

**T**he profound impact of technology and digitisation on how we live and work is sometimes referred to as the new industrial revolution. These new technologies offer huge opportunities and have the potential to solve problems and bring us enormous benefits. But clearly they present risks as well. Commentators including the World Economic Forum have identified rising concern about technology-related risks, including the potential for cyber-attacks on individuals, organisations or infrastructure, data and intellectual property loss, theft and extortion. We're no longer talking just about teenage hackers in bedrooms who can easily be spotted by their masks and balaclavas. Instead we're aware of sophisticated "dark web" operations with their own supply chains, marketing departments and training courses, and probably their own risk management teams too.

So should we all just switch off the computers and go back to paper and typewriters, as the Russian government was reported to be considering recently? Risk professionals have a key role to play in helping their organisations understand and respond to these risks. And the first thing to acknowledge is that cyber risk is just a risk, like any other, and should be managed following the usual principles and processes that will be very familiar to IRM members. Those include a consideration of risk appetite, cultural, behavioural and reputational factors – all looked at in the context of the extended enterprise and supply chains. This process starts with understanding the risks, but what is possibly different with cyber is that many


of us, particularly those of us (dare I say) of a certain age and seniority, are not sufficiently familiar with how our technology actually works. So there is a tendency to leave cyber risk to the IT team – just like we might find a handy teenager to operate the remote control.

Governments and organisations are starting to step up the pace of their response (see *The Forever War* feature in this issue outlining the UK government's developing cyber-strategy).



**So should we all just switch off the computers and go back to paper and typewriters, as the Russian government was reported to be considering recently?**

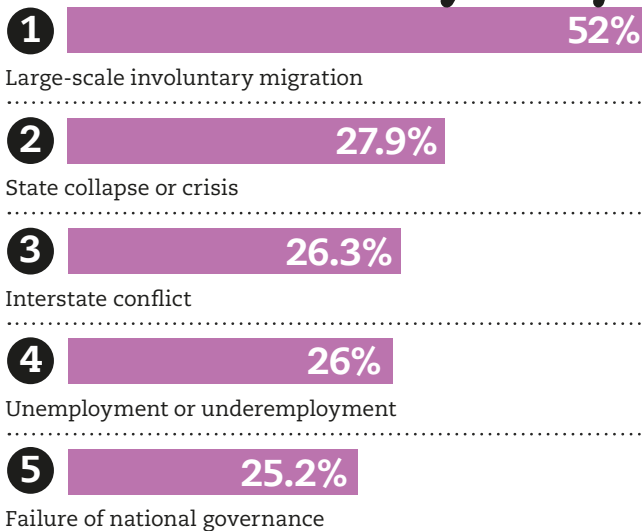
---

My challenge to the risk profession is to encourage everybody to stay relevant and continue to add value by raising our game in relation to technology. You may feel very clever using apps on your smartphone, but do you understand how the coding behind it works and how vulnerabilities might be balanced with customer experience? And do you understand the data flows in your own organisation? And can you communicate these issues to others effectively and participate knowledgeably in discussions about the risks? Expect to see more from IRM, in training, special interest group activity and thought leadership on this subject in the coming months. 

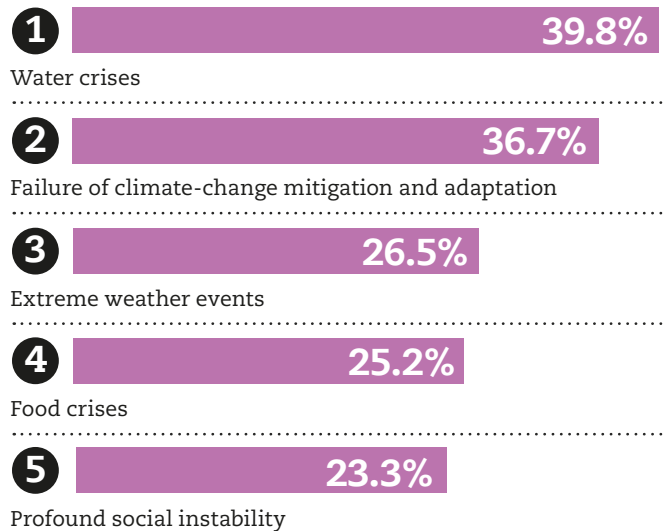
The recurring images of makeshift migrant camps in Europe have dominated the news recently. But in the coming years attention is likely to turn to environmental risk

## Top five global risks

**18 MONTHS** Large-scale migration tops the corporate worry list until mid-2017



**10 YEARS** But over the next 10 years, environment-related risks dominate



Source: The global risks report 2016, 11th edition, World Economic Forum

## Top three global business risks for 2016

**1 Business interruption**  
Including supply chain disruption

**2 Market developments**  
Volatility, intensified competition, market stagnation

**3 Cyber incidents**  
Cyber crime, data breaches, IT failures



38%



34%

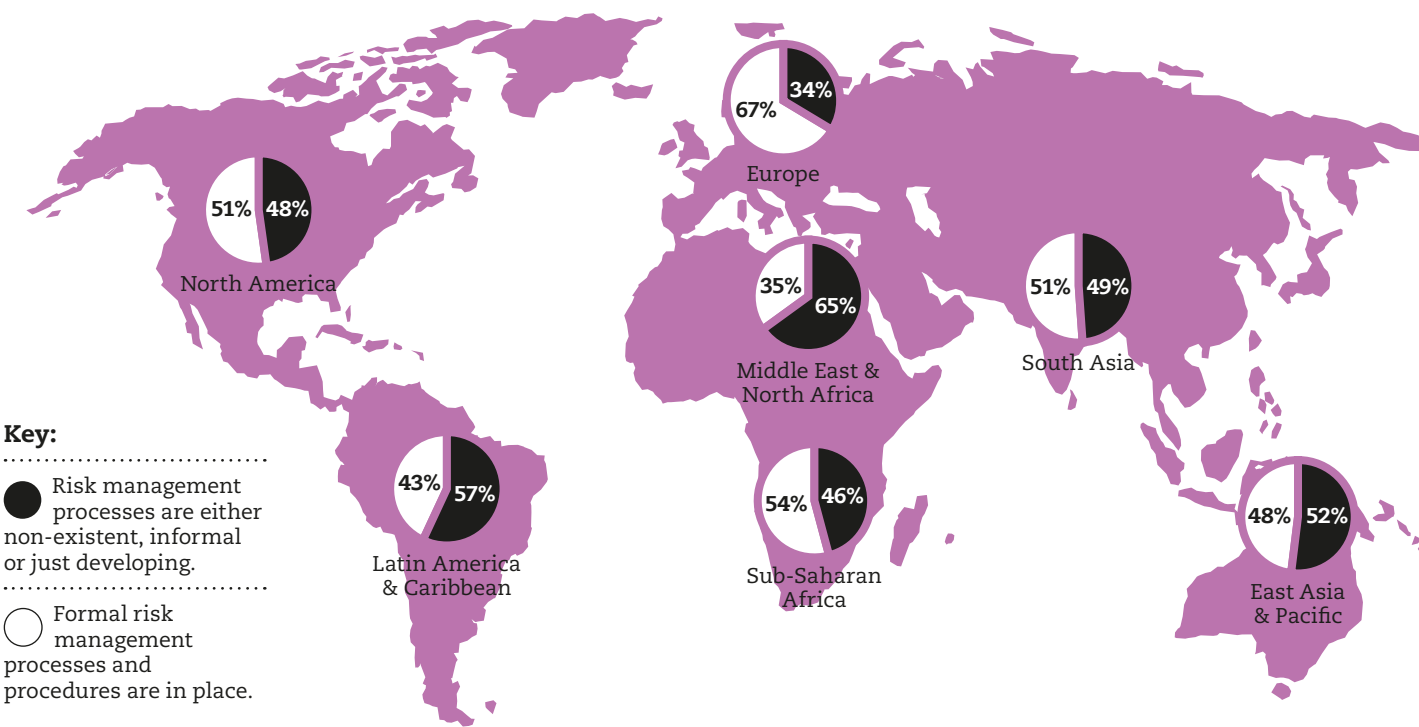


28%

Source: Allianz Risk Barometer – Top Business Risks 2016



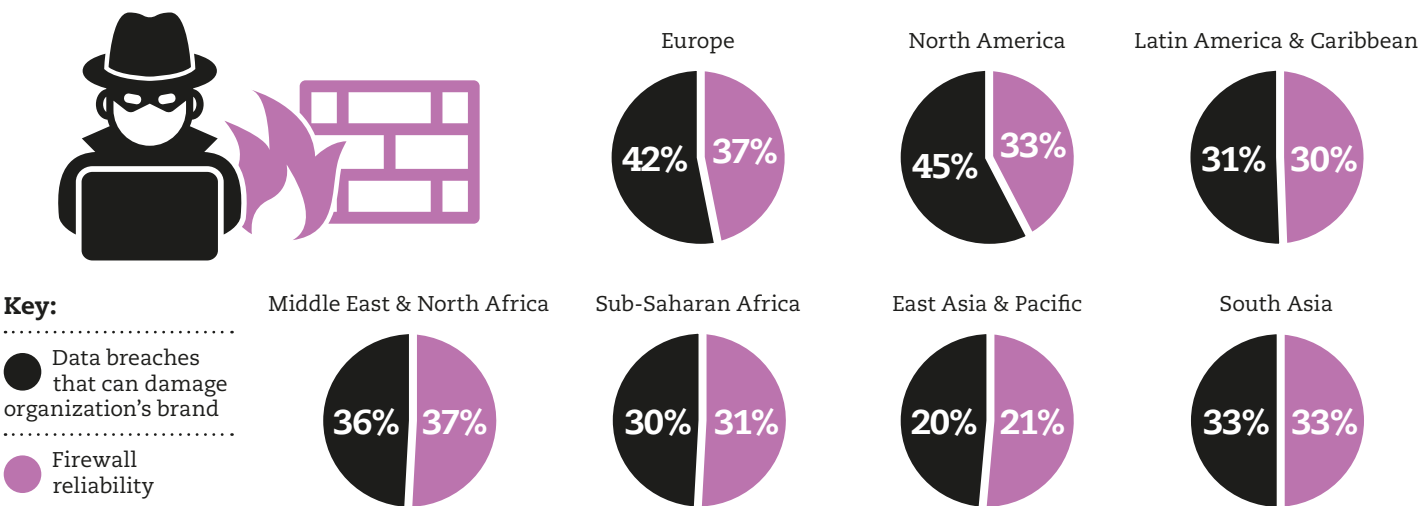
# Europe's organisations lead the way in having formalised risk management processes



Source: Institute of Internal Auditors Global Practitioner Survey 2015 (CBOK)

## Which cyber attacks are most worrying?

Percentage of respondents saying their organisations were at extensive inherent risk – top two categories in each region (choose all that apply)



Source: Institute of Internal Auditors Global Practitioner Survey 2015 (CBOK)

# The Forever War

Stuart Sterling is leading the UK Government's efforts to get the private sector engaged in the war against cyber crime

..... BY ARTHUR PIPER

**T**he cyberwar is escalating. Criminals, nerdy teenagers, state sponsored hackers and hacktivists have never been so busy. According to the most recent Government Annual Breaches Survey, the cost of breaches nearly doubled for large businesses over the last year, with serious security lapses now costing several million. The average cost of the worst incidents to a large business is between £1.46m – £3.14m – more than double since 2014. The biggest losers are UK businesses, according to the research.

The UK government is fighting back. It has spent £860m on the problem through its National Cyber Security Programme over the past five years, with a £1.9bn to come over the next five. But businesses have been slow to seek help and to put in the most basic steps to mitigate the risks of a cyber attack on their organisations.

## Not enough

.....  
“This threat affects all businesses and all businesses, regardless of size or sector or type, should be taking some steps to put cyber security in place,” Stuart Sterling, Private Sector Cyber Security Capability Lead at OCSIA, says. “For that reason, whilst we’ve seen encouraging

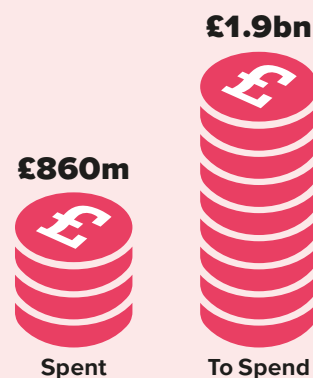


**The fundamental issue is that businesses feel unable to assess the risk**  
.....





## NATIONAL CYBER SECURITY PROGRAMME EXPENDITURE



up-take in things like the Cyber Information Sharing Partnership, we've seen nowhere near the sort of level that we would hope to protect the wider economy."

There is some evidence that businesses are waking up to the threat. The most recent data from the Government's Cyber Governance Health-check Tracker report showed that 88% of FTSE 350 businesses now have cyber on their risk register – that's up from 58% the previous year. While Sterling says that's a good start, he still wants to see more action from businesses – especially small and medium-sized enterprises, which typically have fewer resources.

"The fundamental issue is that businesses feel unable to assess the risk and unless you can assess the risk then you can't take the appropriate mitigations and put those in place," he says. "In many cases businesses don't

know what those steps are."

The Government's Cyber Essentials Scheme aims to plug the knowledge gap and help businesses get the basics in place. They can go through the steps to put the most fundamental controls in place to protect the business and its stakeholders, and they get a certificate at the end of it to demonstrate to suppliers, customers and regulators that they care about cyber threat. Cyber Essentials Plus takes that process one step further.

### Frustrated

"That process can potentially be used as a competitive advantage to show that you take your cyber security information assurance seriously," Sterling says. "The issue is, to be straight, businesses aren't doing this. So with the Cyber Essentials Scheme, we're about to come up to the second

anniversary, yet businesses aren't adopting these simple measures, even though we've provided advice that is recognised as being good."

So while awareness of cyberattacks is growing, Sterling is frustrated that too few businesses are changing their behaviour to meet the threat. Ideally, he would like banks, insurers, customers and others to look at the certificate as an indication that cyber security and information risk is being considered.

"Businesses are failing to see the business benefits of having cyber security in place, which is why we're looking to strategically partner with those influential companies, like banks, insurance brokers, large organisations that have got significant supply chains, professional bodies such as the Institute of Risk Management – all these touch points that businesses come into contact with anyway – and encouraging the same consistent, clear message going out to them, and then that way we should see action," he says.

Risk managers, he says, can help. "There is a significant role for risk managers within their organisations to ensure that there is awareness at all levels of the organisation and that cyber risk is not seen as something incalculable and therefore feared or ignored," Sterling says. He believes from a risk management perspective cyber risk should be looked at in the same way as other more conventional risks. That means understanding





**Above:** "The Doughnut", the headquarters of the GCHQ.

## “Businesses don’t place enough importance on internal preparations and thinking about the actions they take following a cyber incident”

what information is mission critical, assessing the threat from that perspective, and then taking the necessary mitigation steps.

Sterling is understandably reluctant to tell businesses what should be on their risk registers, but cyber risk is likely to affect most either directly, or through their first, second, or even third line of suppliers. He says those risk managers who have still to win the argument that cyber risk should be on their organisation’s risk register can use the Cyber Information Sharing Platform to get the sort of evidence and information they require to make the case to the board that action needs to be taken. “While high-profile breaches raise the attention of the board, being the victim of a breach can be very damaging, not only in cost but in reputation, which can be so difficult to get back after something like that has happened,” he says.

Sterling does not believe that there is a magic bullet to cyber threat

and accepts that no matter what businesses do to protect themselves, there will still be a risk that their organisation’s defences can be breached. That is why defence against potential attack should also include plans for an effective response.

“Incident management planning and exercising should be part of your response to the risk,” he says, “and businesses don’t place enough importance on the internal preparation and thinking about the actions they take following a cyber incident.”

### Essentials

Sterling says that businesses need to make sure their staff have had the right training to cope with such situations. The government has developed free online training courses to help businesses understand cyber crime and online fraud. There are versions for small businesses, for lawyers and accountants, for procurement

professionals and HR professionals.

“So the advice is there, it’s a case of using it and ensuring that, as a business owner, you are taking the steps to ensure your staff know,” he says.

As well as getting up to speed with Cyber Essentials and following the government’s 10 Steps to Cyber Security advice, he says, businesses can contact Computer Emergency Response Team (CERT) direct for advice and help. While Sterling accepts that the Government has still to reach the tipping point where businesses will automatically seek out help and advice in the war against cyber crime, he’s optimistic that the next five years will see positive change in the take up of those services.

As part of the Government’s strategy over the next five years, it is setting up a new National Cyber Centre, which will be overseen by GCHQ. The initiative is part of its National Cyber Security Strategy, which will be published later in 2016. Based in London, the centre is expected to be in the front line of protection for the British people, British organisations, and critical national infrastructure. It will also make sure that local, regional and national public bodies, including all areas of government, know how to be safer on line. Sterling wants businesses to see the centre as their first port of call once it’s up and running later in the year.

“This will bring together all the advice and all the expertise in government into one single front door for businesses,” he says. “Businesses have said that in recognising that there is advice out there, they don’t know where to turn. This will make it easier for businesses so they know where to come and get the right advice for their particular type and sector.”

The Government has also been teaming up with sector specialists to develop and refine its advice. It recognises that the problem is too wide-spread and complex for it to try and tackle it alone. Last year, for example, it established the Cyber Insurance Industry Forum which comprises members of the representative groups within the insurance industry and officials from across government. It follows the success of a similar group in the telecoms sector, the

Telecommunications Industry Security Advisory Council (TISAC), formed in 2009, chaired by the Prime Minister’s Deputy National Security Adviser for Intelligence, Security and Resilience, which shares industry-specific information and best practice.

## Communication

OCSIA is also working with the membership bodies as well, such as the Institute of Risk Management, the Confederation of British Industry, the British Retail Consortium, and the Federation of Small Business. “These groups usefully understand the sector they represent, the type of business they represent and also can help to ensure that the messages and the advice are communicated in the best way that’s likely to see action being taken,” he says.

These initiatives dovetail with the Government’s broader plan to create a community of people who together can make the UK a world leader in the war against cyber crime. The Government is opening two cyber innovation centres, launching a £20m Institute of Coding, providing financial incentives for cyber start-up companies, and partnering with business to boost the country’s skills and capacity in the industry – currently worth about £17.7bn annually to the UK economy.

While the war in cyber space is likely to intensify rather than die down over the next few years, it is true to say that the UK Government has worked hard to put the right infrastructure and systems in place to help businesses win the war. All that remains now, is for companies to join in the fight in much greater numbers. ☎

## CORE HELP FOR BUSINESSES

**Cyber Essentials Scheme.** Helps organisations protect themselves from the most common internet based threats. By getting certified and displaying the badge, it offers a mechanism for organisations to demonstrate to customers, investors, insurers and others that they have taken these essentials precautions. Visit: [bit.ly/1hkkmdz](http://bit.ly/1hkkmdz)

**10 Steps to Cyber Security.** Provides a structured approach for organisations to reduce the cyber risk in 10 critical areas. Visit: [bit.ly/1xnnpd0](http://bit.ly/1xnnpd0)

**The Cyber Governance Health Check Report.** Offers insight into the cyber governance of the UK’s highest performing businesses. It assesses the extent to which boards and audit committees of the FTSE 350 companies understand and oversee risk management measures that address cyber security threats to their business. Visit: [bit.ly/1wglmWs](http://bit.ly/1wglmWs)

**Cyber Streetwise campaign.** Mainly aimed at members of the public, but provides good basic advice for the smallest of businesses and is very accessible. Visit: [www.cyberstreetwise.com](http://www.cyberstreetwise.com)

**The Government’s Computer Emergency Response Team (CERT)** hosts an information and threat sharing platform (The Cyber Information Sharing Partnership) which enables businesses to share current information and experiences to rapidly pick-up on patterns of behaviour and raise awareness. Co-ordinates 4,000 cyber-security professionals from across the country. Visit: [www.cert.gov.uk](http://www.cert.gov.uk)

**Cyber-security Information Sharing Partnership (CiSP),** part of CERT-UK. A joint industry government initiative to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact on UK business. Visit: [www.cert.gov.uk/cisp](http://www.cert.gov.uk/cisp)

**Free training.** Government offers free online training courses to help staff and business owners understand cyber crime and online fraud. There are versions for small businesses, lawyers and accountants, procurement professionals and human resources professionals. Visit: [bit.ly/1Wc7L1k](http://bit.ly/1Wc7L1k)

# Once more into the breach

Cyber attacks can be a nightmare for businesses to prevent, detect and deal with, so why don't organisations put more effort into getting ahead of the game?

..... BY LIZ BURY

So great was the shock of the Talk Talk cyber breach that although it occurred a full five months ago, it's still very much on the tip of cyber risk experts' tongues. The incident was in many ways the stuff of cyber breach nightmares: the hacked customer data, the lack of clear information about exactly what had happened, the CEO Dido Harding rushing between media interviews trying to calm the situation down, the scorn and ridicule on social media, and the tumbling share price. No wonder the memory of it still sends a shiver down most risk professional's spines.

And yet, despite this shocking example of the very real risks of doing business in a cyber-age, many UK companies remain unprepared for a breach. It's not for lack of trying by the UK government, which has worked hard to propel cyber risk up the agenda of UK businesses. Unveiling his new £1.9bn national cyber plan last November, Chancellor George Osborne said: "The starting point must be that every British company is a target, that every British network will be attacked, and that cyber crime is not something that



**Above:** Talk Talk's CEO Dido Harding was thrown into the spotlight during a high-profile hack on the business.





**Above:** UK Chancellor George Osborne says every British company is a target.

**“ Only 35% of c-suite executives believe that their board has a high level of expertise in cyber security**

happens to other people” (See *The Forever War*, pages 10-13).

Still the message is not making it through to some UK boardrooms. Andrew Rogoyski, vice president, cyber security services, at CGI, who spent two years at the Office of Cyber Security and Information Assurance, part of the Cabinet Office, says: “People see high profile cases, and don’t want it to be them, but they struggle, especially at senior level, to know what to do about it. Many are financiers, business people, they know how to deal with the numbers and challenge their management team, but when it comes to cyber security, because it’s a deeply technical subject, they don’t have the language to challenge what they’re being told.”

A new white paper from CGI,

*Cyber Security and the Board*, shows that among c-suite executives in banking, insurance, retail, telecoms, and utilities, only 35% believe that their board has a high level of expertise in cyber security. Such a knowledge gap at the top is a huge challenge and an opportunity for risk managers, as they step forward to help their organisations to achieve greater cyber security.

### Unpredictable

Among the trickier aspects of handling cyber risk is the way in which it changes so quickly and unpredictably. Nick Seaver, partner, risk advisory, at Deloitte, says that this can cause havoc with a traditional risk management cycle.

“The risks are changing really, really fast. In February, we saw a fairly big upturn in distributed denial of service (DDOS) attacks in some industries in the UK, and organisations need to consider very quickly if they have enough resources deployed against a threat that has suddenly increased. The challenge is to be agile enough to respond quickly when the threats change. The cyber attack landscape moves quicker than many risk management cycles within organisations. It just shifts: one month it’s DDOS attacks, another it’s ransomware; things shift around as attackers change their methods and try different things,” he says.

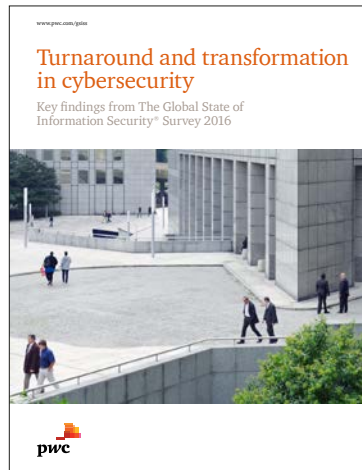
In addition to the changing attack landscape, the risk profile of a company can alter rapidly as

new technology is deployed by the business. “There has been a shift in many businesses, retail is a good example, where they have become more technology focused, with a different risk profile,” explains Chris Gaines, partner, cyber security, at PwC. “New digital systems often come to market at a rapid pace, and in a less structured manner than was traditionally the case, and security is not always fully considered.” A good first step for risk managers in sizing up their cyber risk, therefore, is to acknowledge how adaptable the risk management responses may need to be.

The second big challenge to managing cyber risk effectively is people, and specifically employees. PwC’s *Global State of Information Security Survey 2016*, which polled 10,000 c-suite executives, found that employees topped the list of suspected sources of cyber incidents in the 12 months to June 2015, with 34% of respondents saying that employees were a likely source of breaches. “Too many breaches are because of simple stuff like default passwords, systems not configured securely, and people opening attachments from email addresses that they don’t recognise. There is still a need to get the basics right, and some of the attacks we’ve seen suggest that some organisations haven’t got there yet,” says Seaver. “Anecdotally, I’d say the minority of attacks we read about in the press are of the very complex, that-could-have-happened-to-anyone variety, and the majority are relatively simple things that shouldn’t have been like that.”

## Training

Training staff in the basics of cyber security is a significant step forward on the path to cyber resilience, though it’s not always as simple as it may sound. “A large retailer has staff at its digital business, at head office, in stores, in logistics centres, and they all have very different profiles. It really is a non-trivial task to get security messages that resonate to all those different places,” says Gaines. Phishing, particularly, remains a significant issue for many organisations, and can be especially hard to protect against throughout a large and diverse workforce.



**Above:** Report finds employees topped cyber risk suspects.



**The majority of breaches are relatively simple things that shouldn’t have happened**



The third chunky area for risk managers to explore as they consider how to guide their organisation is network security testing, and response rehearsals. Many organisations today work with a mix of legacy systems and cloud-based services, and rely on myriad networked mobile devices. Tokio Marine Kiln (TMK), a specialist cyber insurer at Lloyds of London, has developed an array of cyber risk management services, including penetration testing, to complement its insurance cover. Justyn Hardcastle, underwriter at TMK, says: “Penetration testing is employing, say, ethical hackers to try to break into the system, work out where the vulnerabilities are, and then help to fix them as well.” Conducting such an exercise suggests that the company has a healthy attitude to understanding its cyber exposure. Says CGI’s Rogoyski: “When you’re ready to test it, you’re in the right place.”

Whereas up until now lots of effort has gone into mitigating the risk of a cyber breach, increasingly firms are testing their post-breach response through a rehearsal exercise. “Run a



## Cyber risk thinking is catching up with health and safety thinking

---

simulation, even if it's just a tabletop exercise," says Seaver. "Get the senior people who would be in the spotlight having to deal with customers, the media, regulators, to rehearse what an attack would be like. Then they've made their mistakes in a safe environment, and they know what to do if it happens for real. It's muscle memory." Certainly the Talk Talk incident might not have struck such a stressful chord if the company's responses had seemed more planned.

With so much to think about and do in relation to cyber risk, and a lively community of would-be hackers out there plotting their next attack, risk managers have their work cut out. The good news is that the thinking around cyber risk is developing fast, and an opportunity for dialogue between risk managers and the board is opening up. Starting with a modest insurance limit can be a useful way to introduce cyber cover and risk mitigation to the board, says Hardcastle: "Boards are still very new to this type of risk, and buying small limits to understand the coverage—how it responds, how it works, what

they can get out of it—introduces an element on which they can build a programme, including risk mitigation services, in the future."

### Response


---

A shift in mindset is already happening at board level, and particularly in the light of Talk Talk, the focus is on breach response. "There has been a healthy change, which moves the thinking from 'we can stop this', to 'we will do everything we can to stop this, but recognise that it might happen anyway'. Much like a plant explosion. Cyber risk thinking is catching up with health and safety thinking," says Seaver.

The other significant change in board executive's minds is seeing cyber as a business risk, rather than a technology risk. This is how the "more mature organisations are starting to treat it," says Rogoyski, adding that, "leadership from the board is essential. It not only tells the outside world—suppliers, customers, shareholders—that it's serious, but also the people

inside the organisation."

The challenge for risk managers is to make their voice heard by the board, and to influence company strategy. Says PwC's Gaines: "Do we know where our sensitive data is stored and what the impact on our brand would be if it was stolen? What security improvements are we planning and what difference will they make? Do major weaknesses exist in our systems and security controls that we need to prioritise? How able are we to identify and respond to a cyber attack?"

He says that these are the questions that risk managers should be able to articulate to the board, and the questions that the board should be asking that person. But, he says, for the most part, many organisations would struggle to answer them adequately. And until those dialogues are taking place frequently and in enough organisations, the breaches that nightmares are made of are likely to continue. 

---

 Liz Bury is a freelance writer.



# White gold's deadly legacy

Controlling the use of hazardous products in developing countries is hard. Businesses, governments and society need to learn the lessons from the global tragedy that asbestos is still leaving in its wake

..... BY NEIL HODGE

**T**he dangers relating to lead paint, asbestos and some pesticides have been known in developed countries for decades, and their sale and use have either been banned or severely curtailed. But when one market closes, others remain open for business and developing countries have long been a lucrative market – as well as a dumping ground – for products that western countries will not touch.

Canadian-based Dominion Colour Corporation, one of the largest manufacturers of lead pigments in the world, is hoping to continue to export paint containing lead pigments from its Netherlands-based plant, despite a ban by the European Chemicals Agency that came into force last May. The company was granted an exemption after it claimed that lead chromate – which the EU added to a list of “substances of very high concern” for human and environmental health – was an essential component of its product. The final decision on whether the company can export its paint rests with EU member states and is expected later this year.

Dominion states that its lead pigments are supposed to be used for industrial purposes only, and that it has strict controls on the companies it is supplying the products to. But industry bodies like the British Coatings Industry oppose the substance's continued use, and over 120 countries have voted to eliminate the use of lead in all paints by 2020 as part of a UN-sponsored



**Top left to right:** Gates of an abandoned asbestos factory in Mumbai, India 2009. An asbestosis sufferer in Ahmedabad, India 2009. An Indian doctor holds a slide of an X-ray showing lung tissue damaged by asbestos exposure, 2009.

**Above:** An Indian asbestosis sufferer holds up medical papers proving his illness is asbestos-related, 2009.



environmental programme.

The World Health Organisation (WHO) says that lead exposure from all products and processes accounts for 143,000 deaths per year with the highest burden in developing regions. Childhood lead exposure is estimated to contribute to about 600,000 new cases of children developing intellectual disabilities every year. The WHO adds that there is no known level of lead exposure that is considered safe, and that lead poisoning is entirely preventable.

## Problems

.....  
 "Lead pigments manufactured in Europe are exported overseas to countries where there are no safety controls and where distribution networks are difficult to check," says Kathleen Ruff, director of RightOnCanada, a Canadian human rights website. She doubts how effective controls over potential risk can be in countries with few

resources to police them.

In fact, campaigners such as Ruff and health experts say that one of the key problems in the fight to ban the worldwide sale of potentially hazardous products worldwide is that the countries where they are being exported to are simply unaware of the risks, or at least their severity. Successful prosecution rates for health and safety and negligence failings are also low, and the chance of suing the parent company based outside of the country is lower still (there have been a couple of successes: in 1997 a group of South African workers won compensation in the English High Court for mercury poisoning, and in 2001 around 7,500 South African workers at Cape won £21m in compensation for asbestos exposure).

Another problem is the fact that hazardous materials are often cheaper than safer alternatives, while aggressive marketing campaigns also pay dividends. In 2009, the *Times of India* ran an advertorial on behalf of

the asbestos industry. Entitled "*Blast those Myths about Asbestos*", readers were assured that "only safe white fibre is used in manufacturing of asbestos cement products in India" and that the "problems" other countries have encountered "are not relevant in the Indian context".

More recently, at a 2014 conference hosted in India by the global asbestos lobby group, the International Chrysotile Association (ICA), Kanat Kapbayel of Kazakhstan's United Minerals (and a ICA board member) said that chrysotile was so safe "you can eat it for breakfast, lunch and dinner". Yet the World Health Organisation's (WHO) position is very clear – all types of asbestos are carcinogenic and that occupational exposure to asbestos causes an estimated 107,000 deaths each year worldwide.

The United Nations (UN) has tried to counter these problems with the formation of the Rotterdam Convention on the Prior Informed



Consent Procedure for Certain Hazardous Chemicals and Pesticides in International Trade, agreed in 1998 and which came into force in 2004. This is a multilateral treaty to promote shared responsibilities in relation to the importation of hazardous chemicals.

## Convention

Under the Convention, extremely hazardous chemicals and pesticides that have already been banned or severely restricted in various parts of the world are put on a special list by the Chemical Review Committee, the Convention's scientific body. Countries must then first obtain "prior informed consent" of the hazards before they can export these products to another country. The Convention also enables countries to have the right to refuse entry of the hazardous product if they believe they are not able to handle it safely.

However, the Convention has its limits – namely, that any substance added to the list must be unanimously approved by all members, and if some countries are host to major producers of the product set to be listed, progress stalls. At the Rotterdam Convention conference last May key asbestos exporting countries Russia, Kazakhstan, Kyrgyzstan, Belarus, Pakistan, India, Cuba and Zimbabwe refused to accept the recommendation by the Chemical Review Committee

to list chrysotile asbestos. Guatemala, Indonesia and India also blocked the listing of paraquat, an extremely hazardous and highly toxic herbicide, that is widely used in parts of these countries.

"By refusing to act, these countries are denying a basic human right – the right to prior informed consent with regard to export of a hazardous substance," says Ruff. "They are denying the right of countries to control their borders, and they are denying the right of countries to protect their citizens from harm."

Baskut Tuncak, UN Special Rapporteur on toxic wastes, went further: "It is both legally and morally unjustifiable for countries to continue to obstruct the listing of asbestos and paraquat under the Rotterdam Convention and derogates from their obligation to realise the right to access information."

The UN has made another notable attempt to encourage companies to act ethically and to take responsibility for their actions, as well as those of companies in their supply chains.

Endorsed in 2008, the United Nations' *Guiding Principles on Business and Human Rights* rest on three pillars of "protect, respect, and remedy" and provide a duty for the state to protect against human rights abuses by third parties, including business, as well as a corporate responsibility to respect human rights. They also provide for greater access by victims to effective remedy, both judicial and non-judicial. These principles have become widely accepted as "soft law", meaning that while they are legally unenforceable, they have become the basis for the expected norms upon which companies operate.

John Sherman, general counsel and senior advisor at independent non-profit organization Shift, which has become the leading global centre for learning and expertise on the UN Guiding Principles, says that companies can – and should – be held liable for dangerous products that they market to countries that either are not aware of the dangers inherent

**Below:** A child plays outside her home where cracked asbestos cement tiles can clearly be seen, 2009.



in the product, or that have low levels of health and safety legislation and enforcement to protect those people that may come into contact with it. He says that a key way to do this is to make organisations more accountable for the actions of their supply chains.

## Supply chains

"A lot of legislation that has recently come into force in the US and EU, for example – such as anti-bribery, corruption and anti-competition legislation – specifically tries to hold a company to account for the actions of third party contractors, suppliers and joint venture partnerships that are acting in its name," says Sherman. "I can see no reason why such concepts are not extended to companies producing and selling substances that are clearly known to be hazardous to health. Furthermore, I think that this is an area that is ripe for negligence claims for western-based companies in years to come," he adds.

Krishnendu Mukherjee, barrister at Doughty Street Chambers, who has worked on over 1,000 asbestos claims involving Indian workers, also believes that it is becoming increasingly common for supply chain



**This is an area ripe for negligence claims for western-based companies in years to come**





“ Companies can do the right thing, and there is a growing realisation that they will need to do so

issues to become part of human rights legislation. Mukherjee points out that Section 54 of the UK's Modern Slavery Act, which came into effect last year, specifically focuses on transparency in the supply chain. The legislation states that companies must disclose in their annual reports what steps they have taken (or not taken) to prevent human trafficking or slavery in their own businesses and their supply chains.

“Given the prominence of supply chains as a key area of risk, I can see no reason why such monitoring cannot be extended to the use, sale or distribution of harmful products in a company's own operations or within the supply chain in the same way that companies now have an obligation to report on what steps they are taking to prevent slavery in their operations and supply chains,” he says.

Some companies have fallen foul of their products being used dangerously and/or inappropriately through their supply chains, and have had to change the way they sell them as a result – winning plaudits for their actions in the process. One example is General Electric (GE), which found that its ultrasound machines were being misused in India to facilitate

female sex-selective abortions – illegal under India's Pre-Natal Diagnostic Techniques (PNDT) Act of 1994, which prohibits the use of equipment or techniques for the purpose of detecting the sex of an unborn child.

As a consequence, GE Healthcare India put in place stringent controls to review its sales process. This included conducting training programmes for sales teams, making amendments to legal contracts, regular auditing, and rigorous sales screening and tracking to verify that the customer has a valid PNDT registration certificate. India's PNDT Act was amended afterwards in 2003 to explicitly recognise the responsibility of manufacturers and distributors to protect against female feticide.

“Companies can do the right thing, and there is a growing realisation internally that they will need to do so,” says Sherman. “It is untenable for companies not to monitor or audit the actions of their supply chains now, and I can't see why the use, sale or distribution of hazardous products or materials should escape scrutiny.”

Neil Hodge is a freelance photojournalist.



**Top left to right:** A boy looks on as his father takes medication to alleviate breathing difficulties associated with asbestosis. An Indian health and safety campaigner holds up an X-ray showing a former worker's damaged lungs.

**Above:** Children make model sculptures from asbestos cement without safety gear, Ahmedabad 2009.

# The bribery conundrum

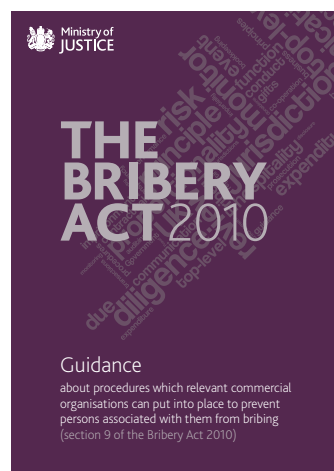
Two recent successful investigations by the SFO have raised questions for risk managers on how and when to report potential bribery misdemeanours to the authorities

..... BY RAY FLYNN

**I**n late November 2015, the Crown Court in London agreed to a 3 year Deferred Prosecution Agreement (a DPA) against ICBC Standard Bank, on the recommendation of the UK Serious Fraud Office, for bribery committed by an Associated Person of the bank's offices in Tanzania. The case involved a payment made by Standard's sister company in Tanzania, Stanbic, to a government official, in order to secure work for both companies.

The DPA was awarded for Standard's forthrightness in alerting the SFO to the offence within days of discovering the transgression and for their agreement to fulfil conditions laid down by the court. Those included paying reduced financial penalties, enhancing their anti-bribery policies and procedures, and to opening themselves up to scrutiny, over a 5-year period, after which any possibility of prosecution would expire. In agreeing to the DPA – the first time such an arrangement has been made under the UK's Bribery Act 2010 – Standard avoided criminal charges and possible debarment from competing in certain markets through being blacklisted.

In February 2016, the Sweett Group, a firm of quantity surveyors based in the UK, became the first company to be prosecuted for the same offence and fined about £2.5m.



**Above:** Ministry of Justice guidance advises businesses to consider getting external verification that their anti-bribery procedures are up to the job.



“ Risk managers should ask an independent expert to cast a critical eye over their anti-bribery systems

No DPA was offered. The court agreed that the company was guilty of “... failing to prevent persons associated with it bribing to obtain or retain business for the company.” So, what are the implications from these two cases for risk managers dealing with bribery risk in their organisations?

### Don't rely on others

The investigations into Standard's misconduct revealed a catalogue of shortcomings in their management of bribery risk. They assumed, for example, that they could leave most of what needed to be done to their sister company in Tanzania, Stanbic, who were the ones who paid a “marketing” fee to a local firm, EGMA, to help them secure the contract. It's worth noting that Stanbic was deemed Associated Persons not by virtue of being a sister company to Standard but simply

because they were helping to secure work for Standard. The judge said the offence was limited to the allegation of inadequate systems to prevent associated persons committing an offence of bribery.

What emerged were several deficiencies in Standard's policies, procedures and controls that allowed this act of bribery to go unnoticed until it was too late. In the end, it seemed that complacency was partly to blame for the error. Risk managers should not rely on related parties to do the necessary work, or on the effectiveness of existing systems. They should test them, preferably using someone independent of the organisation who can cast a critical eye over what insiders might mistakenly consider perfectly adequate safeguards. This piece of advice is given in by the Ministry of Justice in its

document *Bribery Act 2010: Guidance to help commercial organisations prevent bribery*. It states: “organisations might wish to consider seeking some form of external verification or assurance of the effectiveness of anti-bribery procedures.”

### Consider your audience

Both Standard and Sweett were guilty of a Section 7 offence under the UK Bribery Act, which was their failure to prevent others committing an act of bribery with the aim of generating business for the company. However, the Act allows for a “full defence” for the organisation by showing it had “adequate procedures” in place to prevent persons associated with it from bribing, “on the balance of probabilities.” As well as ensuring your organisation has systems in place to prevent bribery, there should



be an element of considering who the audience of these systems might be built into your anti-bribery framework in case you ever have to show that adequate procedures were in place.

The two key elements to this, according to the official guidance to the Act, are the use of risk assessments and an independent review of the systems in place. According to *Adequate Procedures – Guidance to the UK Bribery Act 2010*, published by Transparency International, “An independent review is a best practice procedure. It can provide valuable insight into the strengths and weaknesses of the design and implementation of an anti-bribery programme.” Being able to show that a bribery risk assessment formed the basis of your procedures and that these had been tested independently could amount to a “get out of jail card” where corporate liability is under scrutiny.

### Is DPA the best option?

If they want a DPA, organisations should immediately alert the authorities (the SFO or the DPP in the UK) of any concerns. Do not wait for an internal investigation to reach a conclusion or, worse still, carry out an investigation that convinces you that nothing untoward has occurred.

But there may be times when you should stand your ground and

## Sasi-Kanth Mallela examines the risk-reward equation when considering whether to cooperate with the SFO

What is clear from the DPA Guidance and the Standard case is that a high level of cooperation with the SFO is necessary if you want to be considered for a DPA. That means early engagement and voluntary disclosures to the SFO. Ceding control over your internal investigation, doing what the SFO ask you to do and possibly exposing yourself in circumstances where no prosecution for any offence may have been possible. Whilst it remains a grey area, waiver of legal privilege is also something that the SFO may take into consideration.

Even if you bend over backwards for the SFO there is no guarantee a DPA will be offered. It is for the prosecutor to determine whether it is in the public interest for a DPA to be offered. If the SFO decides not to offer a DPA there is little prospect of having that decision reviewed. You could in your view co-operate fully and still end up being prosecuted. Even if you do get offered a DPA the fine imposed will be the same as that for a guilty plea. Which raises the question – why cooperate in the hope of a DPA?

The DPA process may be quicker at the investigation stage and through the court. If a DPA is entered into and approved by the court it will follow that you receive recognition for your cooperation. This will help you with public relations – you will be able to more credibly represent that you are a reformed company. You will limit the potential for judicial criticism. The Sweett Group received some adverse judicial commentary having pleaded guilty during the sentencing hearing on 19 February 2016.

Whilst you have to agree a set of admitted facts as part of a DPA this does not equate to a formal plea of guilty. This may help limit a company's exposure in related civil litigation and under various debarment regimes, including those relating to EU and UK public procurement

Set against this is the difficulty faced by the SFO in prosecuting



**Right:** Stanbic Bank's headquarters in Tanzania – the sister company of ICBC Standard Bank – where the offence took place.

companies. David Green the Director of the SFO has repeatedly said that this is difficult. In January 2016, for example, he told the London's *Evening Standard*: "If you want to convict a company you have to prove that the 'controlling mind' – usually the board of directors – was complicit in the criminality. That is difficult because inevitably the email trail tends to dry up at middle management and evidentially it is hard to prove". This is why David Green has campaigned for a change in the law relating to corporate criminal liability (who would not want their job made easier?). In weighing

**“ Whilst you have to agree a set of admitted facts as part of a DPA this does not equate to a formal plea of guilty**

.....

up the pros and cons of co-operation risk managers may therefore wish to consider the limited track record of the SFO and other UK prosecutors when it comes to charging companies who, like individuals, are innocent until proven guilty.

It is important to bear in mind that it is easier to prosecute companies under Section 7 of the Bribery Act – the offence of failing to prevent bribery, as the necessary conduct need only have been committed by an associated person and not the controlling mind of the company. This is the offence for which Standard received a DPA and Sweett entered a guilty plea. But where companies are facing other charges are the benefits of a DPA really worth the risk?




**Above:** David Green, Director of the SFO, has campaigned for reforms to criminal corporate liability laws.

risk prosecution. Standard had to pay out a total of nearly \$37m in compensation, penalties, and other costs for a contract where they were expected to share a fee of \$8.4m with their sister company. A DPA or participation in a Voluntary Disclosure Programme is likely to cost an organisation millions of dollars more, in employing a team to investigate other contracts to the satisfaction of their overseers and in

covering the fees of a professional firm appointed by the prosecutors or funders to monitor their controls and activities over a period of years. One of the conditions of Standard's DPA was that they commission an independent review of their anti-bribery systems. For a minor offence, these additional costs could dwarf the potential penalties suffered in the event of a successful prosecution. Regardless, if you feel

your organisation did have "adequate procedures" in place at the time of the act under investigation, this could amount to a successful defence against prosecution. ☞

.....

 **Ray Flynn is an IRM spokes-person and an independent risk management consultant. Sasi-Kanth Mallela is special counsel in the Policy and Regulatory Practice Group at the legal firm K&L Gates.**

**“ Standard had to pay out a total of nearly \$37m in compensation, penalties and costs for a contract where they expected to share a \$8.4m fee**

.....

# Enhance your influencing

Risk managers need to be able to influence those around them if they are to be effective

..... BY RICHARD GOSSAGE



**H**ave you ever wondered how some people just have a way about them, an inner confidence? They seem to get their point across and win the argument – time after time. Have you ever considered why certain chief risk officers (CRO) are so impressive in the risk committee arena, whilst others are just, well, average?

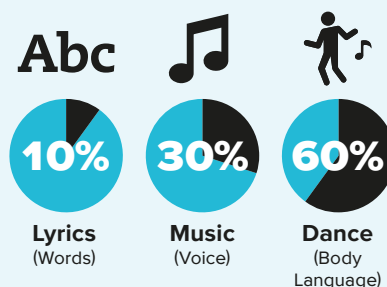
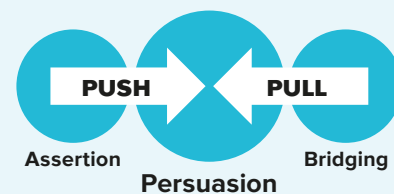
Some are naturally gifted, but in many cases the difference between average and outstanding is the way they apply the professional discipline of influencing.

Through understanding two simple models, and applying the techniques they contain through disciplined practice, you can increase your personal influencing effectiveness materially.

The first model relates to personal influencing, the second relates to strategic influencing. Personal influencing is how you influence another person, a small group or even a large group, in the here and now. Strategic influencing relates to you organising several others to work with you to influence an individual or a group over a period of time. They are inter-related. For example, strategic influencing is less effective if the individuals involved lack strong personal skills.

But let's consider who you may be trying to influence.

## PERSONAL INFLUENCING TOOLS







Let's assume you are a CRO and you have to influence the board, the non-executive directors (NEDs) on the governance committees, the executive, and your team.

We do not spend anywhere enough time trying to understand the world of the people we are trying to influence. Let's focus on NEDs, and specifically chairs of risk committees. How much thought do we give to their wants and needs, the pressures they are under, how they prefer to process and assimilate information, how they are likely to react to what we tell them? The role of a chair of a risk committee is not for the faint hearted. In 2015 APRA, the Australian regulator of the financial services sector, put in place one of the clearest and demanding set of responsibilities for boards and specifically chairs of the key governance committees – search for CPS 220 and CPS 510 on the

**“ We do not spend anywhere near enough time trying to understand the world of the people we are trying to influence**

APRA website to get a flavour. If you want to influence NEDs, walk around for a while in their shoes and design your communications to meet their needs rather than yours.

### Personal influencing

The core model for effective personal influencing is based on two concepts. The first focuses on the influencing spectrum (See *Personal influencing tools*). As the graphic in the top of the diagram shows, the spectrum has persuasion at its centre, and

assertion to its left with bridging to its right. Assertion is a “push” style of influence. It is an instruction – “I want you to...”. Unlike aggression, assertion is a valid form of influencing in society. It is about delivering a fair, balanced message that is unequivocal, not for debate. At the other end of the spectrum is bridging, a “pull” style of influencing. Bridging focuses on influencing through understanding another person's agenda, their objectives, needs and wants. Once you have gained these insights you can work out a “win

win” solution where the objectives of both you and the people with whom you are working are met.

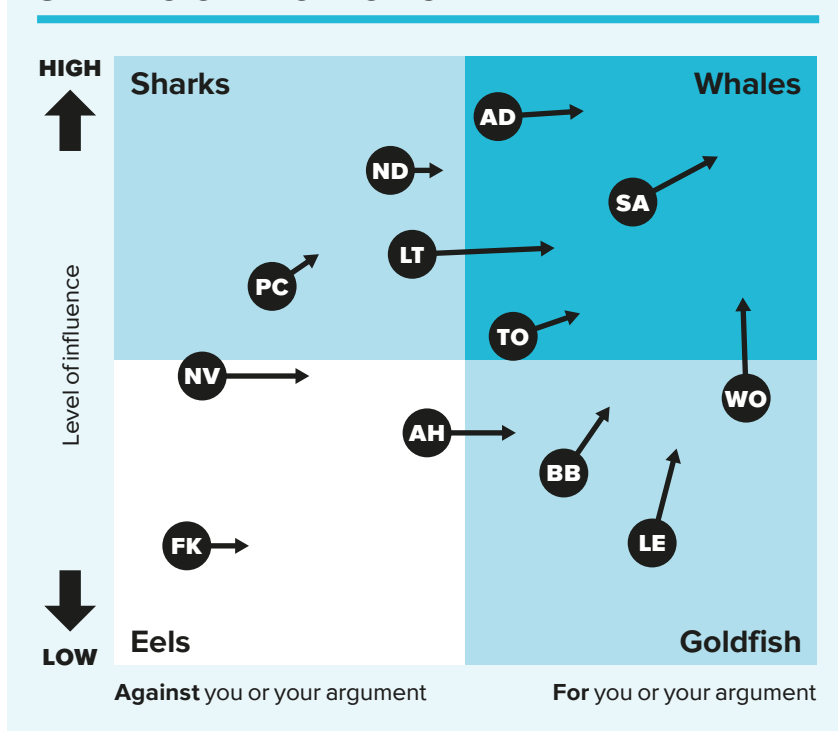
The second concept focuses and what we call the lyrics, music and dance. The lyrics relate to the words that you use. The music relates to the voice; the pitch, tone, loudness, accent used. Finally, the dance relates to the body language that is used to accompany and amplify the message.

To maximise the effectiveness of each type of influencing used there is an optimum mix of lyrics, music and dance; each mix being quite different. For example for assertion the lyrics are minimal, direct. No added or redundant words that detract from the message. The voice is powerful, but not excessive, spoken slowly. Speaking slowly adds gravitas. Introducing pauses after key words turbo charge the seriousness of the message. Just put a two-second pause into the mix and see what difference it makes to the person receiving the message.

In comparison, bridging uses a very different mix. The lyrics are more in the form of questions; ideally open-ended questions followed up by potentially the most powerful question of all, why? Bridging also requires you to actively listen, to regularly summarise, to disclose, and to use silence. Some of us are very uncomfortable with silence but it is a powerful tool to have in your toolbox. Ask a great open question to the chair of the risk committee such as “Why are you feeling concerned about our risk culture?” And then have the confidence to shut up and give the person the time to answer the question. Don’t rush in to fill the space. This is particularly relevant if you are asking someone about how they are feeling about something or someone. The music is a warm, passive voice. It communicates you are genuinely interested. The pace is medium to slow – never fast or loud. Finally, the body language is amplifying your desire to be open and inviting. Palms open and facing upwards universally signals a willingness to listen.

So why does this matter? First, and generally speaking, in one-to-one, or one-to-small group inter-actions up to 60% of the message the recipient takes away is communicated by the body language. Roughly 30% by the voice and a tiny 10% by the actual

## STRATEGIC INFLUENCING MAP



**Some of us are very uncomfortable with silence but it is a powerful tool to have in your toolbox**

words used. Second, people sub-consciously look for confirmation and consistency across the three strands of a communication they are receiving. If the body language is working against the lyrics, the recipient is immediately on guard. Third, make sure you have been understood. Don’t be afraid to ask: “Can I just confirm what you have understood? Have I expressed myself clearly?” Better to ask at the time than to find out someone took away a very different meaning a couple of weeks later.

Before we progress to strategic influencing we need to give due attention to persuasion; the preferred influencing style of the professional. The first stage is to prepare, which means analysing the situation, building a compelling argument and practicing it before you deliver the message. Insufficient time is often given to analysis, undermining the argument – and, all too often, risk managers fail to distil their facts into one compelling argument. In addition, people often fail to practice before the delivery of their argument. Follow up is also key. Not enough focus on recording the results of the meeting and distributing the record to the key people. If you fail to do

this do not be surprised when you learn that everyone who walked from the meeting carried a different understanding of events.

## Strategic influencing

Here are some ground rules. First, strategic influencing can relate to getting a single decision agreed all the way through to developing complex, long-term alliances. The techniques are similar. Second, it is a multi-contact process. This means it requires either you having several meetings with a number of individuals over a period of time, or, more likely, you guiding several

people who are on your side of the proverbial debating table, meeting several others on the other side of the table. Lastly, strategic influencing relates to the structured approach you adopt, but as you move into the plan's execution, it will require you and your colleagues having to deliver strong personal influencing performances to be successful.

To help put this concept across, imagine you are a recently appointed CRO and your aim is to increase the reputation and degree of influence that you and the risk function has in the organisation over a period of 6 months.


Your first challenge is to determine


an assessment of the present – of the key stakeholders who matter, who is pro and who is anti? To help this process the following tool may come in handy. The diagram is a simple 2x2 model with one axis indicating degree of organisational influence and the other indicating whether they are for you, or your argument, or against (See, *Strategic influencing map*).

Being for you and having high influence is where you need a number of the stakeholders to be. These are your whales. We all need a few whales. Against you, and having high influence, are your sharks. You need to know who they are.

For you, but with limited influence are people who are like goldfish – they will keep coming around for a chat, but they are not really going to influence the outcome in the short term. So, don't waste too much of your limited influencing time on goldfish. Against you, but with limited influence are the eels. The trick with eels is managing the numbers. Everyone will have a few and that is okay, but if they start to multiply then you may have a problem.

Having identified your key stakeholders, plot their relative positions by using their initials. This gives you a simple influencing map; your start point. Now comes the trickier part: where do you want those relationships to move to within your first 6 months? A heavy dose of realism is required here. You may want everyone to consider you to be his or her best source of commercial judgement, but it just isn't going to happen.

The diagram shows an optimistic view of the world in 6 month's time – the arrows showing where those people will move to on the map. And now comes the really tricky bit. You have to produce a plan for each stakeholder – represented by their initials on the map – setting out how you, or others on your behalf, are going to influence the relationship to the target position (See *Strategic influencing plan*). Lastly, you have to execute each of the plans. That requires focus and discipline. Nobody said it was going to be easy. 

 Richard Gossage is managing director of Copper Bottom Mentoring, an executive coaching and mentoring consultancy.

## STRATEGIC INFLUENCING PLAN

### Arthur Daley (AD) – Chair of Risk Committee

#### Assumptions

Recently appointed as chair and therefore needs to demonstrate capability to make transition. Needs to create and sell "own agenda". Likely to put his own committee members in place – therefore things will change. Small wins, create momentum, no disasters within first 12 months are core objectives.

#### Influencing Objectives

I need to move to "trusted advisor" status but critically to be seen as company-centric not AD centric. Quality of judgment, pro-activeness, and being seen to do the right thing for company will define my and risk function's reputation. Actions and behaviours rather than words need to drive my thinking.

#### Influencing Approach

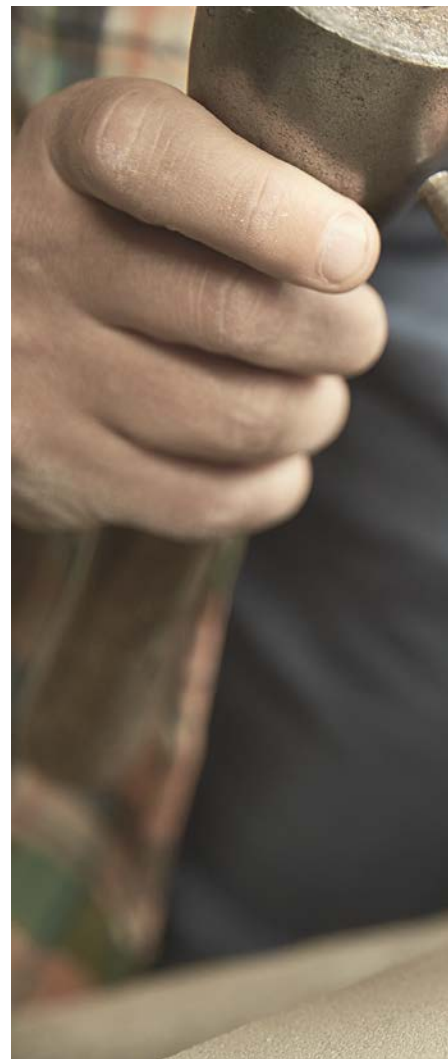
- Be proactive – provide insight and analysis unprompted
- Consult as appropriate, ensure analysis supports better decision making – but be decisive, role model integrity
- Consider unintended consequences – invest time thinking in AD's shoes. Particular focus on AD's relationships – who is he influenced by?
- Get to know AD the person. Use bridging skills to develop an understanding of his values and beliefs
- Avoid situations that put you between AD, the board, and the CEO. Keep personal emotion at bay, promote transparency.



# Written in stone?

Risk managers should not treat an organisation's strategy as though it were written in stone. Applying enterprise risk management to strategy is key to ensuring its success

..... BY AL DECKER AND DONNA GALER



**W**hether an organisation has a formal strategic plan or simply a set of objectives, enterprise risk management (ERM) is a key element of ensuring its success. The strategic plan should outline the strategic thrusts or tactics that have been decided upon; the specific strategic projects in the plan period; and the financial and non-financial strategic goals and objectives.

Once these elements are finalised, it is up those who are responsible for the ERM process to see that risks to these strategy elements are identified, sized, prioritised, and addressed in some way. The alternative ways of dealing with such risks is that they may be mitigated, transferred or accepted, or the strategy may be modified to avoid them. ERM is strategic activity that is meant to address all types of risk across all business functions and activities: strategic and operational, insurable and non-insurable, current and emerging.

Both strategic and non-strategic risks can be significant. However, strategic risks tend to have characteristics which are particularly challenging. For example, they threaten the core mission or product of the organisation, and they are generally not temporary but constitute the on-going



**ERM is strategic activity that is meant to address all types of risk across all business functions**

.....



reality of the future.

A strategic risk might be one that brings uncertainty to an organisation's overall business model, main product or service offering, target customer segment, or basic composition – for instance, an acquisition or merger which carries many unknowns.

For example, the internet has created huge business model risk for many industries. It has either almost destroyed whole industries, such as travel agents, or it has impaired revenue and earnings for other industries, such as retailers, print media, as well as printers. Many other industries are due to be affected, such as healthcare.

When Borders Group, the bookseller, was faced with the strategic risk of changing customer buying habits, it made a number of strategic errors, which made it appear

as if it did not understand the risk at all. Among its strategic errors were brick and mortar expansion in the face of on-line buying, late entry into on-line buying after a profit deflating venture with Amazon and other missteps. These strategic errors in the face of the pressures of trading online contributed to its closure in 2011.

It is important for companies to have robust ERM processes in place for managing strategic risk if they are to avoid similar disasters. It can help organisations overcome such risks by perhaps reinventing themselves to remain viable and profitable.

### In plain view

For the most part, strategic risks are not hiding. They are in plain sight for those who want to see them. ERM is a discipline that enables organisations to identify strategic risks and

## QUESTIONS OF RISK

Ways to identify risks and develop the questions to ask about risk include:

1. Extrapolate from the changing market landscape – how is the future being shaped?
2. Learn from the past – did a certain risk appear before?
3. Note the first warning signal of a trend that carries risk
4. Look at what competitors are saying and doing about risk
5. Discuss market dynamics and risk with professional strategists, academics, and risk experts

to do something about them. Without applying such a discipline, organisations often deliberately or inadvertently ignore looming risk or minimise it because of the lack of systematic ways to analyse it. This can be hazardous to their health.

Within the ERM process there are key steps to be followed. Step one is to list the strategic thrusts and specific goals and objectives of the business. Step two is to ask what risks might affect these. In order for step two to be effective, the leader of the ERM process (for example, the chief risk officer, or risk manager) and those who work with the leader of the process (for example, executive management, or the risk committee) must be knowledgeable about the marketplace and be committed to being honest, open-minded and forthright about risk.

Having these pre-requisites in place, the important questions can be raised and answered. Questions to be asked include: is there a risk that new technology, or a new application of existing technology, will impinge on the organisation's business model? Is there a risk that customer tastes or buying habits will change during the strategic period? Is there a risk that the competition will heat up and create a compelling advantage that is hard to match? Is there a risk that economic conditions will affect the buying capability of customers, or the organisation's ability to achieve sufficient margins?

These questions are asked not out of a sense of pessimism but rather out of the optimistic belief that implementing steps three and four of the ERM process will lead to a more positive outcome. Step three is quantifying the potential impact of the risk, and step four is addressing the risk through one of a number of appropriate means.

### In practice

Let's take the fictitious example of a privately-owned designer and manufacturer of women's apparel and home accessories that begins to see a dramatic and continuing slump in revenue after twenty years of profitable growth. The style of the goods produced is very distinctive and permeates all products. The owners are shocked by the downturn and



**By averting a head-on collision with risk, an organisation may actually be creating new opportunities. This is the elusive upside of risk**

start to frantically make management and other changes. It may be too late.

In an ERM-managed environment, risk to the strategy and goals would have been analysed as they were emerging. Such an analysis would lead to more timely and more effective actions.

If the organization's strategy was to maintain a single design style (which also represented the brand), then the risk-related questions to be asked could include: is there a risk that social or cultural changes might affect our customers' buying preferences or needs? Is there a risk that new styles among competing products will eat into our market share? Are there any market statistics that show there is already a new style among competing products that is already capturing market share from us? Is there a risk that we have reached buying saturation where everyone who wants our products has some?

### Addressing strategic risk

Of course, it is not enough just to identify the risks to a particular strategy or strategy element. An organisation must decide how to address those risks. But before





## THE DIFFERENCES BETWEEN RISK MANAGEMENT AND ENTERPRISE RISK MANAGEMENT

### Risk management

1. Addresses primarily insurable risks
2. Lacks major focus on strategic risks
3. Is most concerned with annual insurance programme renewals
4. Is more internally focused
5. Lacks multifunctional leadership and is more siloed
6. Does little to promote open dialogue and risk awareness

### Enterprise risk management

1. Addresses both non-insurable and insurable risks
2. Focuses on the strategic risks and how to manage them
3. Is a continuous loop
4. Is internally and externally focused
5. Involves multifunctional leadership through an ERM committee, for example
6. Promotes an open dialogue and risk awareness


that can be done, the risks must be evaluated as to how likely they are to materialise and how much of an impact they could have. An organisation cannot typically afford to address all the small risks which might exist. And it must keep some sort of balance between what a potentially large risk may cost versus what amelioration of risk will cost. But without both sides of the equation, identification and action, ERM will not create real value.

Once the most serious risks are identified and agreed upon, the organisation can focus on a response. The ERM process guides the organisation to the point of action but management, the risk owners and staff professionals, must supply the expertise for appropriately addressing risks.

As with any risk, there are several ways to deal with strategic risk. The organisation can take measures to reduce, transfer, accept the risk or avoid the risk by virtue of modifying the strategy. By averting a head-on collision with risk, the organisation may actually be creating new opportunities. This is the elusive upside of risk.

For example, if an organisation identifies the risk that new

regulations will cause it to substantially change the composition of its product, it may spur innovation to create a more popular, safer and perhaps even less expensive formula for creating a replacement product well ahead of the competition. In fact, innovation is one way to deal with many of the strategic risks that have surfaced in the current marketplace. Innovation labs, creative centres and think tanks are quite prevalent. For example, the insurer Aviva recently opened the second such enterprise (its first is in London) – a 'digital garage' in Singapore. The garage is a dedicated space where technical specialists, creative designers and commercial teams explore, develop and test new insurance ideas and services. The project is meant to make financial services more tailored and accessible for customers – but it is also a key testing ground for future strategic direction and risk. With so many new technological advances in progress, strategic ERM is more vitally important than ever. ☞

 Al Decker and Donna Galer are the authors of *Enterprise risk management: straight to the value* published by ERMSTTP, 2015. [www.ermsttp.com](http://www.ermsttp.com)

**“ Innovation is one way to deal with many of the strategic risks that surface**



# Get the Recognition You Deserve

Continuing Professional Development (CPD) is relevant and applicable to all IRM members, whether you are studying, qualified, working part time or undertaking a career break.

Being a risk professional brings with it a responsibility to maintain your competency by ensuring your technical and business knowledge and skills are relevant and up-to-date.

Maintain and enhance your knowledge and skills to complement both your current role and your future career progression.

## What's in it for you?

A planned, structured approach to your own personal development will help you:

- Learn new skills and keep up-to-date with the latest trends
- Perform better in your current role
- Gain a competitive edge and improve your future employment opportunities
- Increase your self-confidence
- Enhance your professional reputation
- Achieve tangible evidence of your commitment, competence and professionalism

Ultimately CPD will help you to attain Certified Member status and keep you current and competent.

Compulsory from 1st July 2016.

**Contact IRM for further details or visit:**  
[www.theirm.org/membership/continuing-professional-development](http://www.theirm.org/membership/continuing-professional-development)



## RISK LEADERS 2016



**Have you got the strength, stamina and flexibility to deal with the all the challenges of tomorrow's risk landscape?**

Find out at IRM's Risk Leaders, to be held in London on 24th November 2016. Now in its 7th year, the conference convenes top risk professionals, board members and governance experts to share case studies, best practices and practical next steps to help you define, achieve and sustain a high-performance risk management program now and in the years ahead.

You will learn strategies to success as a CRO, share and gain experience of how boards work, an understanding of principal risks and long term viability statements, get a fresh look at risk, regulation, and enjoy a unique opportunity to network with senior risk professionals.

## KEEP LEARNING

**Sign up for the IRM's continuing professional development (CPD) programme.**

It is a lifelong process of learning and continuing personal development. It's the means by which you can maintain and enhance your knowledge and skills to complement both your current role and your future career progression.

IRM members are responsible for deciding themselves what and how much CPD activity to undertake in any year. It helps you learn new skills, keep up-to-date, improve your performance, gain a competitive edge in your career, as well as enhancing your professional reputation and providing tangible evidence of your commitment, competence and professionalism.

## CERTIFICATION

Become a Certified Member (CMIRM) and join an elite community committed to maintaining the very highest standards in risk management. Acquiring the qualification will enable you to use the Certified Risk Professional title and the designatory letters CMIRM to show others that you are an up-to-date, experienced and qualified risk professional.

Visit the IRM website for more details on CPD and certification.

## SLAVERY IN THE SUPPLY CHAIN?



**Recent reports allege that Nestlé and Jacobs Douwe Egberts may have inadvertently used slave labour due to the source of unknown beans ending up in their coffee. It is reported that they do not know the details of exactly who works on the plantations in their supply chain.**

Dr Ian Livsey, Chief Executive of IRM, says: "All businesses are under a legal obligation to be able to check and verify the robustness of their supply chains. It is imperative, especially given the recent launch of the recent Modern Slavery Act 2015, that businesses consider supply chain risks as part of their enterprise wide business models."

He adds: "There is always scope for inappropriate behaviour where people and processes are involved and our stance is that these vulnerabilities should be considered as part of risk modelling to protect human rights as part of the overall risk management strategy".

Dr Aidan McQuade, director of Anti-Slavery International, writing in a joint statement published with IRM, says: "Nestlé's confirmation of forced labour being present in the production processes of its products looks to be indicating a growing tendency amongst businesses towards greater transparency in their supply chain."

He said it opened the possibility for greater collaboration between business, civil society and government to work together to confront the risks for businesses in relation to forced labour.

"It feels like a good moment for such collaboration, with the Modern Slavery Act in the UK putting an obligation on businesses to report on what they do to tackle slavery in their supply chains. It will help them to work with organisations like ours to better understand the problem and help reduce the similar reports in the future," he adds.

IRM will be launching its *Bribery Guide* in the coming months.

## RISKS TO WATCH

### OIL

Uncertainty in oil price will be a key issue in 2016 that will affect investments and operations, according to Mark Boulton, IRM Fellow and director at NNV GL, the consultancy. "Even with the forecast increasing demand for oil, it's expected that supply will continue ahead of demand in the short term," he says. Financial commerciality risk for operators will remain heightened by sustained lower prices and uncertainty – meaning operators in high cost fields could fail and the supply chain contract further. Expect possible political instability.

### AUSTERITY

The healthcare and charity sectors in the UK are continuing to feel the squeeze from constrained or reduced budgets. The impact of changes to staffing costs mean that increasing numbers of doctors are leaving the NHS, says healthcare consultant Patrick Keady. In the charity sector, cuts to Local Authority funding for charities could result in some failing, says IRM's Charity Special Interest Group member Alyson Pepperill.

### BUSINESS MODELS

Tech-powered financial services businesses could disrupt traditional business models in the financial services sector, says Alex Hindson, Chief Risk Officer at Argo Group International Holdings.

For more IRM predictions: <http://bit.ly/1P01AI2>



## Insurance claims handling and risk management software



JC Applications Development Ltd is a market leader in the development and implementation of highly effective Risk Management and Claims Processing software. With over 25 years experience and a strong presence in both the Public and Commercial Sectors, our entire team is focused on ensuring that our risk management and claims management solutions are richly functional, cost effective, fit-for-purpose and with great support. We provide scalable, intuitive solutions for risk management, governance, and claims management that really work.

 **Phil Walden**  
 **+44 (0) 1730 712020**  
 **phil@jcad.co.uk**  
 **www.jcad.co.uk**  
 **JC Applications Development**  
**Manor Barn, Hawkley Rd**  
**Hawkley, Liss, Hampshire**  
**GU33 6JS**

## Risk management technology



Riskconnect is an independent innovator and the only global provider of enterprise-wide risk management technology solutions. Built on the world's leading cloud platform, Riskconnect breaks down silos and unites the entire organisation by providing a holistic view of risk management. Through Riskconnect RMIS, Riskconnect GRC, Riskconnect Healthcare, and Riskconnect Safety, the company provides specific and configurable solutions needed to reduce losses, control risk, and increase shareholder value. Riskconnect's growing suite of risk management applications are built on a lightning fast, secure, and reliable platform you can trust.

 **Ross Ellner, Director, EMEA**  
 **+44 (0) 7714 262351**  
 **ross.ellner@riskconnect.com**  
 **www.riskconnect.com**  
 **Riskconnect Ltd.**  
**52 Kingsway Place**  
**Clerkenwell**  
**EC1R 0LU**

## Risk management software



Magique Galileo provides flexible and fully integrated web-based solutions for enterprise risk management, policy compliance, incident management, questionnaires, issue tracking and extensive reporting. Its web interface works with PC, laptop, iPad and other smart devices, enabling the whole organisation to participate in the risk management and assurance processes.

 **Trevor Williams or Verna Hughes**  
 **+44 (0) 203 753 5535**  
 **info@magiquegalileo.com**  
 **www.magiquegalileo.com**  
 **Magique Galileo Software**  
**Level 30, The Leadenhall**  
**Building, 122 Leadenhall Street,**  
**London, EC3V 4AB**

---

## Specialty insurance solutions

---



Allied World Assurance Company Holdings, AG, through its subsidiaries and brand known as Allied World, is a global provider of innovative property, casualty and specialty insurance and reinsurance solutions. With 20 offices servicing clients throughout the world we are building a global network. All of the Company's rated insurance and reinsurance subsidiaries are rated A by

A.M. Best Company and S&P, and A2 by Moody's, and our Lloyd's Syndicate 2232 is rated A+ by Standard & Poor's and AA- (Very Strong) by Fitch.

**Rachel Pankratz**  
 **+44 (0) 207 220 0630**  
 **rachel.pankratz@awac.com**  
 **www.awac.com**  
 **Allied World**  
**19th Floor, 20 Fenchurch Street,**  
**London, EC3M 3BY**

---

## Risk management information systems

---



NTT DATA Figtree Systems is a specialist software provider for risk management Information Systems. Figtree Systems is used globally for incident and OH&S management, claims management, corporate insurance and employee benefits management, fleet and asset management and enterprise risk management. By using system features such as workflow automation, document

management and creation, reports and dashboards, smartphone and web-based data-capture and email notifications, users have reported increased productivity, lowered costs and improve risk management processes. Easily configurable, the system is available in the traditional client-server model as well as a Software as a Service (SaaS) model from ISO 27001 compliant datacentres.

**Ayaz Merchant**  
 **+44 (0) 20 722 09210**  
 **ayaz.merchant@nttdata.com**  
 **www.figtreesystems.com**  
 **NTT DATA Figtree Systems**  
**Level 3, 2 Royal Exchange,**  
**London, EC3V 3DG**  
**United Kingdom**

---

## Risk management training

---



As the world's leading enterprise risk management institute, we know what great risk management looks like, and what risk management professionals need to know, do and deliver to succeed. What's more, we understand how training works and we are experts in designing and delivering courses that provide the tools and motivation to make change happen. Our short

courses and tailored in-house learning and development solutions support hundreds of organisations every year, both in the UK and internationally. Some courses, like the Fundamentals of Risk Management, cover the broad range of ERM skills, whilst others take an in-depth look at specific topics, e.g. Risk Analysis, Risk Appetite and Tolerance, Managing Risk Culture, and Identifying Key Risk Indicators.

**Sanjay Himatsingani**  
 **+44 (0) 20 7709 4114**  
 **sanjay.himatsingani@theirm.org**  
 **www.theirm.org/training**  
 **IRM Training**  
**Sackville House,**  
**143-149 Fenchurch Street,**  
**London, EC3M 6BN**

---

**To advertise here contact:** Clementina Christopher ✉ [clementina.christopher@theirm.org](mailto:clementina.christopher@theirm.org) ☎ +44 (0)20 7709 9808

# Is the rate of change really accelerating?

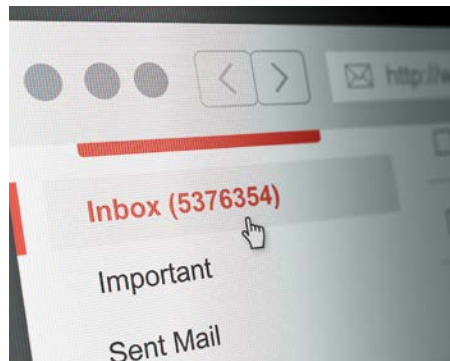
*While white collar workers feel swamped by a tsunami of emails and media, there seems little empirical evidence to suggest that the nature of change is speeding up*

Thinkers began to realise in the 1960s and 1970s that the nature of change was undergoing profound change. Alvin Toffler – famous for his book *Future Shock* and after whose spirit this column is named – was among the first to ponder what an apparent acceleration in the rate of change would mean to both businesses and the people who worked in them.

Businesses would become more transient, be subject to rapid growth and unexpected disintegration, and people, he said, would feel increasingly disorientated in a world that technology had fundamentally transformed. They would experience the same kind of shock independent travellers feel when they encounter cultures they have never visited before, he said.

Forty-six years later, it may seem that Toffler's future has arrived. The number of column inches newspapers devote to how companies such as Google, Facebook and the fledgling Uber are disrupting the world as we know it are vast. People speak of their children as "digital natives," or "millennials," because they have grown up with information technology and seem to have a far deeper and more intuitive grasp of its potential than the culturally-challenged over-50s. And, finally, people cannot keep up with the blizzard of email, social media feeds, 24-hour rolling news services and other sources of information they feel obliged to consume.

Risk managers have undoubtedly been swept up in this torrent of excitement and are busier and in more demand than




Even though the processes about which you know more are not inherently moving faster, seeing them in far greater detail makes it feel as if time is speeding up

ever. All well and good. But less well remembered is Toffler's second insight – that change occurs unevenly and the impact of technological development is non-uniform. Leading risk executives may be jetting around the world in their information-rich environments, but less than half of the world's population have access to the internet. Furthermore, even within organisations, project timeframes are often very different – some rapid,

others snail-like. Too much focus on accelerated change in technology-centred projects can blind risk managers to the fact that much slower rates of change are both normal and valid elsewhere. Just because there is a blizzard of information on all fronts does not mean there is a global storm blowing strongly everywhere.

Research published by *The Economist* in December last year, "Time and the company," said that CEOs now receive on average between 200-400 emails a day, giving the illusion of acceleration in all dimensions of life: "Even though the processes about which you know more are not inherently moving faster, seeing them in far greater detail makes it feel as if time is speeding up," it said. *The Economist* found no real quantitative evidence of such acceleration over the past 10 years in key business indicators – from the average tenure of CEOs and staff, to manufacturing inventory days and the duration of corporate bonds.

The lesson for risk managers is to understand that change is accelerating in some parts of the economy, but not in all, and certainly not evenly. Risk from slower developments – climate change and human life-expectancy – can be profound and need as much, if not more, consideration than those that grab our immediate attention. The key is to understand what the significance of the rate of change is for the part of the business under review. That's why the notions of speed and change need decoupling if we are to understand the potentially different impacts they can have on organisations. 



# irm Global Risk AWARDS 2016

## 15 April 2016

Venue: Park Lane Hilton Hotel, London.

## AWARDS DINNER celebrating success

IRM's fourth annual Global Risk Awards.  
Our entrants are internationally recognised  
for their excellence in risk management.

visit us at [www.theirm.org/GRA2016](http://www.theirm.org/GRA2016)

## Book Your Table

### Prices:

#### Tables of 10

Table(s) of 10 for awards entrants: £2995+VAT

Table(s) of 10 for non-awards entrants: £3495+VAT

#### Individual Dinner Places

Individual Dinner Places for awards entrants:  
£325+VAT

Individual Dinner Places for non-awards entrants:  
£375+VAT

#### Booking & Sponsorship Opportunities

Clementina Christopher, Sponsorship & Advertising  
Manager

t: (0)207 709 9808

e: [clementina.christopher@theirm.org](mailto:clementina.christopher@theirm.org)

400 guests 40 countries 13 categories 1 amazing night

Headline sponsor



Platinum sponsor



Award sponsor



Award sponsor



In association with



# Minimise your business risk.

## Consult a specialist.

Working with brokers and clients, our dedicated team of experts have in-depth industry experience and a thorough understanding of the issues facing your sector. We thrive on delivering a truly personal service, and coming up with flexible, innovative solutions that transform your business by making it more risk aware and helping to improve your bottom line. Visit [www.QBEurope.com/rs](http://www.QBEurope.com/rs) or email us at [enquiries@uk.qbe.com](mailto:enquiries@uk.qbe.com)

**Business insurance specialist**

QBE European Operations is a trading name of QBE Insurance (Europe) Limited and QBE Underwriting Limited both of which are authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. QBE Management Services (UK) Limited and QBE Underwriting Services (UK) Limited are both Appointed Representatives of QBE Insurance (Europe) Limited and QBE Underwriting Limited.