

Enterprise Risk

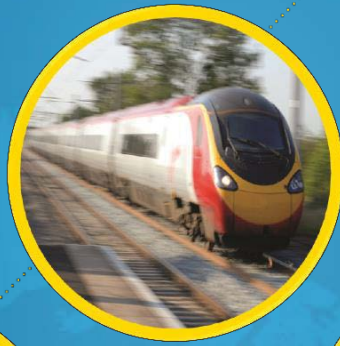
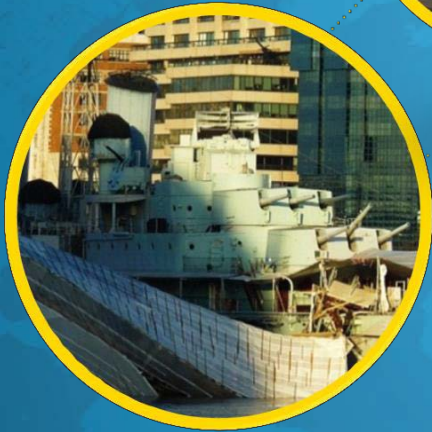
Summer 2017 / www.enterpriseriskmag.com

The official magazine of the Institute of Risk Management

Risk agenda 2025: the big debate / **Fintech challenge:** new kids on the block / **They're here:** hack attack / **Planning for success:** project risk / **Predictably vulnerable:** why safe businesses fail



Living on the ceiling: Iain Wright joined Old Mutual Wealth at a time when the business and the industry were undergoing rapid change



Leaders in forensic investigation

Hawkins is a well-established firm of forensic scientists and engineers. Founded over 30 years ago, we have eleven offices spread across the UK, United Arab Emirates, Singapore and Hong Kong. We employ over 80 highly skilled investigators.

We cover a broad range of investigations and our clients include insurers, loss adjusters and the legal profession. Our service is both independent and impartial.

Please call us on +44 (0)20 7481 4897
to discuss your requirements
or visit our website:
www.hawkins.biz

Investigations include:

- Personal injury
- Road traffic accidents
- Engineering
- Highways
- Contamination assessment
- Escape of water, fluids and gas
- Railway accidents
- Fire and explosion
- Power generation
- Civil & structural engineering
- Shipping & marine

Hawkins
Leaders in forensic investigation

Editor

Arthur Piper

Produced by

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, 143-149
Fenchurch Street, London, EC3M 6BN
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



The benefit of inaccurate polling

As I write this, millions of Britons are schlepping through the rain on their way to the polling booths for the UK general election. I opted for the dry – in both senses – option of postal voting.

Predictably, there have been thousands of floating voters. They appear on TV and in opinion polls as those who haven't yet made up their minds. By the time you read this editorial, they will have done so and the results will be in.

Following the disaster that was the psephology of the Brexit campaign predictions, the polls this time around have played with different methods. Some have even given the Labour leader Jeremy Corbyn a lead – most don't.

Is psephology in crisis? That seems to be the consensus. But it is worth remembering that this has been the consensus since about 2,000 and before. Polls never get it right about the future. In fact, they seldom get it right about the past.

You would have thought that most people could remember how they voted in a general election. According to a poll conducted three weeks after the 2001 election only 26% remembered having voted Conservative (7% too low), while 48% said they had voted Labour (6% too high).



It's not only the future that is liable to bias when it comes to polling accuracy, it is also the past

So, it's not only the future that is liable to bias when it comes to polling accuracy, it is also the past.

In many ways, this inaccuracy about what people think their intentions or performance is likely to be is useful to risk managers. Even if some of this slippage between talk and action can be put down to groupthink – where people in well-defined social categories, such as boards, tend to have the same views – it can still help risk managers root out problems.

What really matters in opinions is not the difference within the groups, but between them. Take corporate culture, which is increasingly subject to surveying techniques. It doesn't matter if the general view is that the business' culture has been poorly communicated across the organisation. It does matter if the board thinks it has and nobody else agrees. Or if risk managers think they are providing cutting edge services while the ship is sinking. Anthony Fitzsimmons and Derek Atkins writing in this issue of the magazine – *Predictably vulnerable*, pages 28-31, have interesting insights into resolving those issues.

Improvements to corporate culture, risk management and other business areas are best achieved by providing a critical perspective – even if that perspective may not be accurate by any objective measure. The UK's would-be prime ministers worked harder and harder as the polls narrowed, even though those polls were probably mostly inaccurate.

Arthur Piper

Editor

Looking for a better way to manage risks or audit?

Currently using a spreadsheet with a small budget and understaffed?

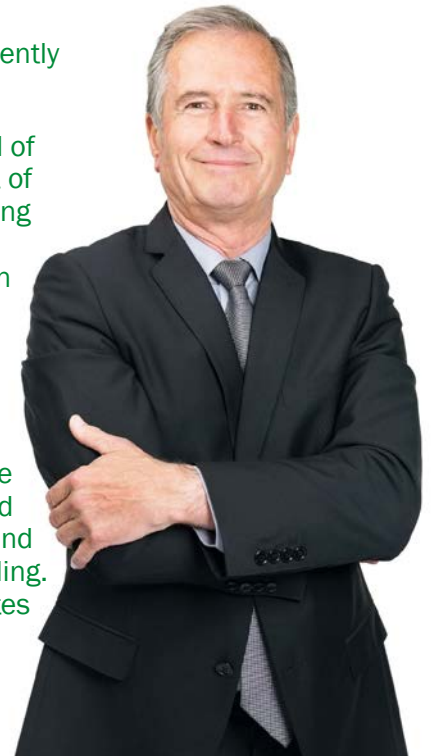
Take a look at Symbiant

“Having previously managed all our Corporate risks via spreadsheets we are currently migrating our risk registers onto the Symbiant Risk Management System.

The capabilities of the software are allowing us to considerably enhance the level of risk maturity across the University. It is allowing us to transform the management of our organisational risks to the extent that our Risk Management Policy is now being reviewed to ensure it takes into account the potential of the new software. As a Higher Education Institute our risks are, on-the-whole, assessed and evaluated on a qualitative rather than quantitative basis – Symbiant is able to accommodate this and allows us to clearly link risks to our non-financial, academic objectives.

Symbiant is also proving highly customisable to our needs with staff finding the user interface intuitive and familiar. This has considerably reduced the training and support burden as we roll it out. The extremely comprehensive reporting suite allows our schools and business units far more freedom and scope to identify and record their local risks since the large amounts of data generated can be easily and almost instantly reported upon in many ways including heat maps and colour coding. This is enabling our risk management to become far more comprehensive. Updates and improvements to the software are regular and reliable with Symbiant having introduced some minor requested enhancements within just a few days”

*Phil Boshier - Strategy Development Officer
Cardiff Metropolitan University*



The Total Risk, Audit and Compliance Software solution

Symbiant is an award winning modular solution that allows the whole workforce to collaborate on Risk, Audit and Compliance issues with prices starting at only £300

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



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

www.symbiant.uk

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

Symbiant[®]
Better Software



10

FEATURES

10 Living on the ceiling

Iain Wright joined Old Mutual Wealth as its first group CRO at a time when the business, its risk management structure and the industry were going through rapid change

14 Perspectives on the future of risk

In the first of a two-part report on the IRM's Risk Agenda 2025 initiative, we look at what key industry professionals say about the future

16 On the road

In the second of our two-part report of the IRM's Risk Agenda 2025, we look at the progress of the big debate as it makes its way around the globe

18 Challenges of fintech

A new breed of financial technology is shaking up the industry, but it's not all plain sailing

21 They're here

Hackers can and do penetrate most IT systems. But organisations are getting smarter

24 Planning for success

Risk managers can make a crucial contribution to the success of new business projects

28 Predictably vulnerable

Why do seemingly sound organisations unexpectedly fail?



14



16

REGULARS

07 Chairman's message

The research into the possible directions the profession will take in future has got off to a good start

08 Trending

The stories and news affecting the wider business environment as interpreted by our infographics team

33 IRM focus

A report from the IRM's 30th Anniversary celebrations at Zurich Risk Engineering

38 Directory

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

38 Toffler

Whistleblowers occupy a strange place in corporate culture. They are the good guys who nobody likes



18



21



24



28

Do you have a Real-World Interface?



riskHive's new 'Real World Interface' for the riskHive ERM application links to and monitors any number or type of external data sources and connects them as Key Risk Indicator (KRI) inputs to warn of or trigger automatic risk response processes. From negative tweets to dipping rates to weather warnings. We've got it covered.

riskHive ERM is a secure, simple and highly configurable ERM Portfolio solution that aligns to and helps define your processes, delivers instant results, requires minimal formal training and scales-up effortlessly.

Whether you're just starting-out on your risk journey or are already expert and require more advanced capabilities the riskHive ERM solution will help ensure a successful implementation of your ERM strategy.

“We demand a return on investment for all our systems. Choosing a risk management system was no different, and we selected riskHive on the grounds that they were able to demonstrate to us that they understood exactly what we were looking for and we had the confidence that they would deliver. They have not only delivered, but continue to engage with us to enable us to drive our ERM agenda.”

Rebecca Cope-Lewis DipQ MCQI CQP CIRM
ERM Director, Mitie Group PLC.

Find out more at www.realworldinterface.com
or contact us for a demonstration of riskHive

info@riskhive.com
+44 (0)1275 545874
+44 (0)781 8898997
www.riskhive.com



Your profession needs you



The research into the possible directions the profession will take in future has got off to a good start. Clive Thompson urges you to get involved

We are now seven months into the IRM's ambitious *Risk Agenda 2025* project, which, as most of you will know, aims to help map the future of our profession. Key stakeholders have shared their views for our report *Perspectives on the future of risk*, and members have been meeting around the world to provide fresh perspectives. Our special feature on pages 14-17 gives a flavour of the both of those initiatives.

It is too early to come to any firm conclusions, of course. Not only are the roadshows still rolling, but members and professional bodies with an interest in risk have been completing our *Risk Agenda 2025* online survey. If you haven't already filled it in, you can find it on our website.

Not surprisingly, though, the risk profession looks set for a period of further change. Not only are new technologies transforming the way that risk managers can harness developments in big data, risk analytics and artificial intelligence to improve their depth of sight, but the speed of change in business models, digitalisation and macro-economic factors mean that new risks are emerging thicker and faster than ever before.

It is only part of the answer to turn to these technologies as the solution to the future of how our profession will work. They will play a huge part in how risk can be identified, quantified and managed – not just defensively, either, but to provide businesses with competitive advantage and agility.

Yet it can be too easy to get mesmerised by the potential transformative power of technology. If we put all our eggs in that particular basket, we will not only need to


watch the basket but we will have to watch for the unintended consequences too.

What we need to tease out is an understanding what type of professionals we will need to become to thrive in the challenging world that is arriving. What skills and competencies will we need? What relationships will we need to build and with whom? The answer to those questions will form a key part of the route to our future success.



We need risk professionals to tell us how they see themselves both now and in the future

And for that, we need risk professionals to tell us how they see themselves both now and in the future. I would urge you to get involved and have your say, if you haven't already. The questions we have posed in the *Risk Agenda 2025* project are crucially important to us all. And we need everybody to play a part in imagining a way forward that will make the risk profession more effective and relevant than ever.

We will be releasing findings at the IRM's Risk Leaders conference in November, so please play a part and, if you can't get to the conference, watch out for the findings soon after: www.theirm.org/thebigdebate 

Clive Thompson is Risk Agenda 2025 Chair and Senior Projects Director at Willis Towers Watson

The latest stories and news affecting the wider business environment as interpreted by our infographics team

Companies are out of step with consumers on data privacy

Despite progress in risk management methodology and investment in sophisticated software programs, finance professionals believe it's going to get tougher to forecast risk



Customers and companies see the business' obligations on data differently



Organisations have an obligation to take reasonable steps to secure personal information



Organisations have an obligation to control who has access to personal information



How customers react to a data loss

Lose trust in the organisation



65%

Discontinue relationship with the organisation



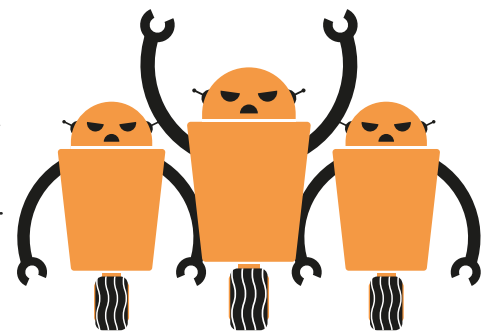
27%

Suffer loss through criminal activity



11%

Source: *The Impact of Data Breaches on Reputation & Share Value: A Study of Marketers, IT Practitioners and Consumers in the UK*, a Centrifry/Ponemon study, 2017



Customer fears about the rise of AI

What people worry about, when they worry about artificial intelligence



33%

AI is never going to know me and my preferences as well as a human being



24%

The rise of the robots and enslavement of humanity



10%

I'm finding that I get on better with AI than with friends and family



5%

Robots are uncovering my deepest secrets



28%

Not worried

But most people don't know they already use artificial intelligence

34%

People who think they have interacted with AI recently



84%

People who have actually interacted with it

Source: What Consumers Really Think About AI: A Global Study by Pega

Clerical workers face brunt of job losses from automation

Percentage of jobs at risk of disappearing because of automation in the UK by 2030

Clerical and support workers



53%

Trade work and elementary work



45%

Services and sales



28%

Overall UK



30%

Source: Will robots steal our jobs, PwC research

Living on the ceiling

A year ago, Iain Wright joined Old Mutual Wealth as its first group CRO at a time when the business, its risk management structure and the industry were going through rapid change. How did he fare?

..... BY ARTHUR PIPER

When Iain Wright accepted the position of Chief Risk Officer at Old Mutual Wealth's office in London last year, he knew it was going to be a challenge. The company's £9.5bn London-listed parent company

Old Mutual Plc was in the process of breaking up into four legally separate entities spanning Africa, the USA and the UK. That would most likely result in Old Mutual Wealth seeking its own listing on the London Stock Exchange, and required a complete shakeup of the organisation's risk management function.

"From being in an environment where we have a group risk function at the PLC level and risk managers in each of the underlying businesses," he explains, "I came in to build a group risk function at the Old Mutual Wealth level."

It has been a big job. Old Mutual Wealth has several divisions which oversee about £122bn in customer investments (See *Old Mutual Wealth structure*). The businesses include investment advisory services, discretionary fund management, a technology platform business, asset management and an international arm. Naturally, there is a huge level of regulatory oversight from the Financial Conduct Authority, the PRA and overseas regulators. And Wright came in when a major upgrade of its adviser technology

OLD MUTUAL WEALTH STRUCTURE

- Old Mutual Wealth UK** – wealth management
- Old Mutual Global Investors** – asset management firm
- Intrinsic** – financial adviser network
- Old Mutual International** – cross-border investment provider
- Quilter Cheviot** – discretionary investment management firm
- AAM Advisory** – offshore advisory service





I came in to build a group risk function at the Old Mutual Wealth level

.....



platform was already underway.

Wright was either wise enough – or crazy enough – to start with a blank sheet of paper and work from first principles.

Vision

.....
“The first thing to do was to define the vision, set out the vision to my team and stakeholders and appoint my senior management team,” he says. If that sounds like a big task for one person, Wright’s approach is fundamentally collaborative. Talking with other risk leaders and executives in the business, they came up with four main purposes for the risk management function.

First, it needed to provide the business with consistent insight and challenge. Second, effectively advise and support the business and strategic decision making. Third, give assurance that customer and shareholder interests are protected. Finally, build

trust with internal and external stakeholders through consistent delivery and high performance.

The second stage was to think how that could be achieved in reality. Given the first two aims, Wright and his team decided it would be no use having a centralised risk function sitting remotely from the business. “One of my stated visions for risk at Old Mutual Wealth is that we are one function supporting one business,” he says. “We are structured so that the risk functions sit alongside the relevant businesses and are made up of risk professionals with expertise of that particular industry.”

When it came to recruiting – a process that has been prolonged and, of which, more later – that principle was put into practice. For example, the CRO of Intrinsic – Gill Davidson, who Wright appointed and joined the team in 2016 – is both a seasoned risk

person and someone who has worked in a variety of advice businesses. At Old Mutual Global Investors, CRO Jessica Brescia, a risk professional who has been with the firm since 2009, has deep experience in asset management businesses.

Given their backgrounds and experience, it makes sense for Old Mutual Wealth’s CROs to sit on their divisional executive management committees – as does Wright at Wealth Group – providing oversight and challenge on a real-time basis. That co-operation between risk and the company exists at all levels of seniority.

Organise

.....
The next decision was how to organise the team – which resulted in creating two distinct streams within the risk management functions of each business. Just less than one third

“ One of my stated visions for risk at Old Mutual Wealth is that we are one function supporting one business

of the 130 people who work in risk at the firm are dedicated enterprise risk management professionals. The remainder work in regulatory risk, which includes fraud and terrorism.

Wright spent a lot of time talking and visiting people. He shared the collective vision for and structure of the risk function with his team, various stakeholders within the company – including Paul Feeney, the Chief Executive Officer of Old Mutual Wealth – the Board and the regulators. Each group needed different handling. For example, the Board needed to understand that Wright’s proposed mission and structure had a clearly defined logic that would be right for the business.

He decided to keep in close contact with the regulators. “We have a very clear interest in making sure we can provide evidence to the regulators that we have a robust risk management framework,” he says. “It’s better to keep them up-to-date with the journey and get their views, than to present them with a big set piece at the end.”

Given the amount of collaboration he decided to seek, it wasn’t an easy process. He laughs with some relief when he tells me that the last of the senior appointments has just been made. And he admits that his reluctance to compromise on the quality of people has made the recruitment search longer than he had perhaps anticipated. He obviously wanted people who had relevant business knowledge and experience, technical expertise, but also people who would be able to interact and communicate effectively with management. The difficult part was getting people with the mix of all three attributes.

“I don’t want a group of people who sit in an ivory tower and when they talk it is all risk mumbo-jumbo,”

he says. “I want people who can interact and talk the language of other people.” That meant he was prepared to bring people in from the business and train them up. Eventually, he would like to see people circulate in and out of risk from all parts of the business – something he describes as “an end game.”

Industry

Globally, he sees technology and regulation as the two main driving forces of change within financial services. Cyberattacks and data security are obvious threats, especially since hacking has turned from a cottage industry in the 1990s to big business, which is often state sponsored or carried out by criminal gangs hoping to hit the jackpot. “It’s not anything new,” he says, “these threats have been around for quite a while. But we need to make sure there is continual reinvestment and focus in these areas.”



The company has also been investing in its customer- and adviser-facing technology platform. Old Mutual Wealth had been developing a replacement platform with provider IFDS for three years when Wright arrived. It wasn’t working out despite being £330m into the project. So, the company looked to see if an external supplier could build a tailored solution that would work.

“We found it relatively easy to find a provider for the kind of platform we wanted,” he says. “Technology has moved on so much from the time we started creating our own platform that it’s now possible to buy something at lower cost that does a good job. That hadn’t been available three years earlier.”

Old Mutual Wealth appointed FNZ in an £160m deal. While the backend of the IT solution is relatively standard and complies with regulatory standards and customer requirements, Old Mutual Wealth focused on creating a customer-facing



CURRICULUM VITAE IN BRIEF

Iain Wright joined Old Mutual Wealth as Group CRO in 2016. He came from Sun Life Financial where he had been senior vice president, enterprise and operational risk. He was chief risk officer at Prudential, UK and Europe.

Wright started out as a chartered accountant with the accountancy and consultancy firm Deloitte. He moved from there to the London Stock Exchange where he worked as head of equity and debt markets. When the Financial Services Authority was formed in 2000, Wright headed up the supervision of major insurance groups.



We have a very clear interest in making sure we have a robust risk management framework

.....

experience that has its own look and feel and that makes a difference to the way their advisers can work.

He believes that changing regulatory requirements have created opportunities for Old Mutual Wealth too. The number of advisers serving customers has fallen in the UK since the financial crisis, and banks have withdrawn services in these areas. Old-style insurance products are on the decline as customers look to new wealth management options driven, in part, by relaxed pensions regulations and a move to simpler, more transparent products. Coupled with increasing customer appetite for managing their affairs online, he is optimistic about the future.

"We have a platform that wins awards for its service levels, but that is an entry point," he says. "We are constantly thinking about how we can continue to differentiate and demonstrate value added in our service and products."

But given the diverse nature of the

organisation's business, regulatory pressure from changes to the relevant regimes is significant.

"It is difficult to argue with much of the regulatory change, but the volume and diversity make it a challenge," he says. As well as industry-specific regulation, such as Mifid II, new European data protection laws – known as General Data Protection Regulation – require all companies to introduce stricter controls on data privacy, with eye-watering fines for those who get it wrong. In practice, that means financial services firms have increased investment in staff who manage that regulatory change – both in the risk function and in the first line of business where the change must happen.

Never dull

.....

"Part of the thing about working in the risk function of a financial services organisation is that it's not a dull

place to be," he says wryly.

He would like to see the continued professionalisation of risk, which is one of the reasons he accepted the invitation to join the Board of the Institute of Risk Management recently. While he is a great supporter of the IRM's qualification program, he also warns those coming into the profession today to be inquisitive and gain new experiences outside their immediate expertise.

"People of my generation often came into risk accidentally with a range of experiences behind them," he says. "Younger people taking a qualification should seek experiences outside of that formal education. We need to contextualise an awful lot of information and that's hard to do with a narrow range of experience."

And would he recommend risk as a profession? "We're fortunate to be in an environment where risk is a very dynamic profession, risk is continually evolving and we're all learning. It's a great culture to be in." 📱

Perspectives on the future of risk

The risk profession is at a crossroads according to leading stakeholders. In the first of a two-part report on the IRM's Risk Agenda 2025 initiative, we look at what key industry professionals say about the future

..... BY ARTHUR PIPER

For risk professionals, it is both the best of times and the worst of times. The best, because in many organisations risk is now highly valued and resourced. Chief risk officers work closely with the board and executive management on strategic, operational and emerging risk projects. And new technological tools promise to help risk managers see trends and threats earlier and in more detail.

The worst, because the profession could be relegated to a back-office compliance function. If heads of risk fail to deliver the value their businesses expect, they face being replaced by automated systems with risk leaders remote from the board and decreasingly relevant.

The stakeholders taking part in the IRM's recent Risk Agenda 2025 report *Perspectives on the future of risk* were both supportive of risk professionals and cautiously optimistic. But all saw the need for improved performance from risk departments if the potential benefits of future risk management practice were to be achieved by 2025.

Mark Brown, vice president of software solutions and services at Sword Active Risk – the project's technology



Above: Perspectives on the future of risk report.



partner – said that risk managers needed to make the case that they exist to foster business growth and are not just there to help with compliance and governance. “By taking a proactive role in promoting business change and opportunity, risk managers will benefit the business and raise their profiles within the organisation,” he said.

One key role that risk managers could play is to be a catalyst for information sharing on risk across the entire business, he believed. “The only real way of succeeding in an environment where everything is a lot tighter financially and moving much faster, is for information to be shared,” he said. “The CRO will oversee the enterprise-wide sharing of comprehensive risk intelligence

“ My challenge to risk managers is to identify the right metrics and data and turn them into the information non-executives need to perform their roles effectively

that will enable the organisation to take advantage of opportunities proactively, locking in profits identified in the business case, as well as mitigating risk.”

Unthinkable

Dame Judith Hackitt, chair of the UK manufacturing body EEF, agreed. Using new technologies and enterprise-wide knowledge, risk managers should focus on the near unthinkable. “The only way to try to manage the future is to be horizon-scanning, be forward-looking and to work through scenario plans – no matter how unlikely those events seem,” she said. “Using the past as a predictor of the future is definitely old hat and risk managers need to grasp that reality.”

Gabriel Bernardino, chairman of the European Insurance and Occupational Pensions Authority (EIOPA) said that risk management was evolving positively in many insurers, but the situation was a work in progress. Solvency II’s Own Risk and Solvency Assessment (ORSA) has highlighted some areas where current risk management practice could be improved.

“There is often a lack of deep analysis and work in areas such as operational risk and reputational risk, which tend to be much more qualitative,” he said. He believed it was critical for risk managers to get out of their comfort zones and tackle these issues. “This kind of risk management requires a more in-depth understanding of the business itself and an increasing need to go beyond pure financial risk,” he said.


Participants in the project agreed that risk managers would have more data than ever before. While big

data and analytics will make the information available to the board more comprehensive, for example, it will also be potentially less helpful. “One of the most important parts of the risk manager’s job in future will be to reduce the tsunami of data into something that is manageable and useful,” Peter Swabey, policy and research director at ICISA: The Governance Institute, said. “Going forward, my challenge to risk managers is to identify the right metrics and data and turn them into the information non-executives need to perform their roles effectively.”

Closer relationship

Many chief risk officers and risk or audit committee chairs would need to develop a closer relationship for this to happen. “The periodic appearance of the chief risk officer in front of the board is a good thing. It’s an opportunity for the board to make clear what information it wants,” he said.

Mark Goyder, founder and chief executive at the business think tank Tomorrow’s Company agreed that the relationship between the board and risk management would need to strengthen. “In future, the board needs to be the risk committee and the risk manager the specialist who is clearly focusing the board’s mind on risk and helping foster a risk mentality.” Getting the culture right will not be easy. But with the proper focus, some smart thinking and courage, risk managers in 2025 could be realising their potential to truly enable the success of the businesses they serve. 

 **Further reading:** *Perspectives on the future of risk* bit.ly/2rDCHPV

On the road

In the second of our two-part report of the IRM's Risk Agenda 2025, we look at the progress of the big debate as it makes its way around the globe

..... BY CAROLYN WILLIAMS

We kicked off our big debate at the IRM's flagship *Risk Leaders* conference in London in November 2016. This annual event is aimed at those concerned with risk at board level and the issues emerging clearly reflected this top-level view.

Delegates told us that they were currently taking steps to better understand the interconnections between their risks and how these might play out. Many were looking at improving their risk reporting, with some starting to examine real-time monitoring solutions. Some wanted to find better ways of identifying the value that risk management added to their organisations.

Many delegates were excited by the potential for using big data techniques, artificial intelligence and machine learning, and predictive analytics for managing risk in future. Some thought that the risk team of the future would be a small central unit, focusing on supporting strategy and on building and embedding risk management capacity across the organisation.

Africa

.....
Following our conference in London, we met with risk professionals in Nairobi in Kenya, Harare in Zimbabwe and Johannesburg in South Africa. At the first meeting of our new, Kenya Regional Group, attendees agreed that they were



Top to bottom: Zimbabwe, Belfast, Kenya, Switzerland, Kuwait, South Africa.
Top right: Uganda.



Skills in analytics and horizon scanning as well as soft skills, such as influencing and change management, would be vital for future risk professionals



as global issues, such as technological advances and climate change. Development of skills in analytics, horizon scanning as well as soft skills, such as influencing and change management, would be vital for future risk professionals, they believed.

We returned to Africa in April 2017 when we visited Kampala in Uganda. Delegates there welcomed the opportunity to talk about the challenges of introducing and integrating ERM. A wide range of projects were under way ranging from the development of policies, indicators and quantitative techniques, as well as work looking at the impact of organisational culture.

Looking to the future, they agreed that significant upskilling, training and capacity building was vital if organisations were to take advantage of the opportunities offered by digitisation, to support commercial success and also meet the challenges of global risks. There was also an expectation that risk awareness would need to be built across organisations, not just in the risk team.

Europe and the Middle East


In March 2017, in a joint session with Chartered Accountants Ireland, we met in Belfast in Northern Ireland. Risk managers there – many from the public sector – said they were currently focusing on fraud, health and safety, environmental issues and data protection. Some organisations were starting to think about integrating risk and opportunity management, tackling strategic risk, and rolling out work on risk appetite and risk culture into the wider organisation.


By 2025, our Irish delegates thought that a mixture of technology, training and culture change could

potentially make everyone a risk manager. In particular, organisational and individual skills needed to be developed in horizon scanning, use of technology and social media. Improved risk management capability could potentially lead to greater risk retention and the need for more innovative risk transfer products, they said.

Our group in Zurich in Switzerland said risk managers were currently focused on streamlining, strengthening and improving the efficiency of their relatively mature risk management processes. They agreed that standardisation of procedures and using the best tools and techniques to improve the quality and reliability of information were important. In future, the risk function could become more creative and people-focused – the human touch supervising largely automated systems for monitoring risk.

In Kuwait City in Kuwait, most attendees worked in the oil and gas sector. They felt strong pressures to demonstrate the value of risk management and its contribution to the success of the organisation and to project delivery, they said. Some were embedding various aspects of ERM – from integrating risk into decision-making, to process improvements and some initial work on culture and behaviour. Budgets were an issue, but they believed that ERM would remain a focus for their organisations going toward 2025.

Over the coming months, we will be continuing the debate on the future of risk. Please get involved either by attending one of our forthcoming workshops and by filling in our survey. 

 Carolyn Williams is the IRM's Director of Corporate Relations. Get involved at: www.theirm.org/thebigdebate

currently searching for better ways to analyse and report on risk. Work was underway, they said, introducing formal risk management processes, policies and frameworks into many public and private organisations.

While risk maturity in many organisations was lower than at our London gathering, effective risk management was perceived as a vital tool in both building the economy and dealing with issues such as climate change, power supply and infrastructure. Risk managers in larger organisations, such as those we met in Zimbabwe over breakfast, said they were working to improve their risk reporting and analytics. They expressed enthusiasm for new ways of working and expected the public sector to increasingly adopt risk-based thinking.

At our South Africa Regional Group, attendees said that the prospects for their region posed a particularly high level of uncertainty going towards 2025. That meant organisations needed to be prepared for local challenges as well

Challenges of fintech

A new breed of financial technology is shaking up the industry, but it's not all plain sailing

..... BY NEIL HODGE

The rise of financial technology – or fintech – firms may well be both a blessing and a curse to traditional financial services providers. While some of these new starters have set themselves up as challenger banks to sell and deliver fairly simple financial products quickly and easily to a growing population of tech-savvy customers, others have taken the route of selling their services to existing players, enabling banks rather than competing against them.

Experts say that fintech firms have much better customer interface tools and customer relationship management (CRM) programmes and, because they can analyse customer behaviour via social media, they have a much broader understanding of what customers want. That enables them to sell more products with larger profit margins. Furthermore, traditional banks and insurers are in danger of being left behind in the race to digitalise services.

“Traditional financial services providers need to embrace fintech more rapidly to accelerate their digitalisation plans,” says Bertrand Lavayssiere, UK managing partner at financial services consultancy Zeb. “Traditional banks and insurers are hampered by



Traditional banks and insurers are hampered by their legacy systems and cannot easily make the transformation to increase and improve their range of digital services

.....



If a fintech firm gets hit by a cyberattack, it can be over – the whole business premise is built upon transacting quickly and safely online

professional risk managers employed by global financial institutions.

Some fintech pioneers believe that the new entrants can teach their traditional rivals some lessons in how to improve compliance. Kevin Wilbur, senior vice president, accounts payable automation at e-invoicing fintech company Tungsten Network, believes that “fintech companies find it easier to ensure full compliance” because “we don’t have to operate using legacy systems that simply aren’t fit for purpose. All our processes are built from scratch to be transparent and agile. The truth is fintech is what helps businesses be compliant.”

Wilbur also believes that traditional banks and insurers can learn from the way fintech firms are managing risks. “By adopting a digital approach and automating core business processes, compliance is far easier to achieve, as paper-based invoice processes make it difficult, if not impossible, for businesses to ensure they are compliant,” he says.

Cross over

On the other hand, there is a lot of knowledge sharing between the two sectors. Romi Savova, chief executive officer and founder of PensionBee, an online pension manager that enables people to find and then combine their old pensions into one plan, formerly worked in the risk management department at global bank Goldman Sachs. She is well-versed in the approach that large, traditional financial services firms take towards risk and compliance. “Many of the large company practices have stuck with me and have influenced the setup of PensionBee,” she says.

Savova says that fintech firms need to manage the same sorts of risks as big financial services companies, and that “fintech firms are held to an equal standard as regulated firms”. However, she adds that “it is important to note that traditional banks and insurers have diverse lines of business and the

compliance requirements on those firms are reflective of that.”

For example, she says, capital and reporting requirements are more onerous where customers are relying on product guarantees – and for good reasons. Different lines of business also come with the potential for conflicts of interest, where one arm of the business is acting in a way that furthers the commercial interest of another department – at the expense of the customer. While these risks can present themselves for fintech companies too, Savova says those business models are usually simpler and more focused. “This setup makes the risks more apparent and therefore, in many ways, easier to manage,” she says.

Downsides

On the flipside, if something goes wrong at a fintech company, it can be substantially more damaging. “There is less history there to create a ‘context’ for what has happened,” says Savova, “and to provide confidence that the fintech company can manage through a problem. That’s why risk management should be on the top of every fintech CEO’s agenda.”

Ali Alani, CEO at Imperial FX, a fintech firm that specialises in foreign exchange and remittance, agrees. “It’s imperative that leaders within fintech firms fully understand risk management. At the end of the day, managing risk is at the core of financial services, and fintech isn’t excluded from this.”

Alani says that the key compliance and risk management issues that are at the top of his organisation’s risk agenda are enhanced due diligence, anti-money laundering and terrorist financing procedures. “It’s business critical that these are enforced,” he says.

“We are required to keep records of transactions that date back five years and all clients must be checked against a number of sources, such as the EU sanctions list, and lists issued


by the Office of Foreign Assets Control and the Financial Actions Task Force. Given the current political turbulence, you can see how this is a demanding task – but one that is fundamental to the business,” says Alani.

As fintech is synonymous with cutting-edge technology, Alani says that a key aspect of any risk management approach must also mean “identifying any risks, or opportunities that present themselves with emerging technologies.” He also believes that those responsible for managing risk need to work closely with the product and operations sides of the business “to ensure a seamless customer experience.”

Real time

Fintech customers expect real-time responses to their requests, such as for loan approvals, which means that risk management must be able to assess risks automatically. To achieve this, says Alani, fintech firms are using modern intelligence such as social media behaviours and spending history to analyse credit risk and target profitable customers, while algorithms – which can be used for underwriting, monitoring and fraud detection – and machine learning are being readily used to reduce operational risks including human error and cyberattacks.

Matt Stanton, head of business intelligence at IT provider Synectics Solutions, says that although fintech companies’ technology may be cutting-edge, the investment in cybersecurity measures is nowhere as much as traditional banks are spending. “If a bank gets hit, it can deal with the fallout, however bad,” he says. “If a fintech firm gets hit, it can be over – the whole business premise is built upon transacting quickly and safely online.”

There is little doubt that much of the innovation in the financial services space is being driven by the fintech revolution – and that sound risk management will be at the heart of its success. While the banks and new entrants fight it out, customers will continue to go where they can find the best returns at a level of risk that suits them. 

 Neil Hodge is a freelance journalist



Image credit: IBM Research

They're here

Hackers can and do penetrate most IT systems. But organisations are getting smarter too, according to speakers at ISACA's recent conference in Munich

..... BY ARTHUR PIPER

Towards the end of this year, we could reach the point at which quantum supremacy has been demonstrated. If you have never heard of it, you should pay attention now. It marks the date when scientists will have built a quantum computer that has the potential to be more powerful than any other supercomputer on the planet. It could also mark the date when the encryption that most businesses use to protect their important data becomes useless.



Given the user address for a Bitcoin, for example, a quantum computer could work out the security code that protects the money from being stolen in a couple of minutes

.....

CHALLENGES TO QUANTUM-SAFE SECURITY

- It takes several years of cryptanalysis for cryptographers to gain confidence in the security of new algorithms
- Some network security protocols may be too rigid to accommodate the increased key lengths or changes in ciphers required to make them quantum-safe
- New standards for protocols are needed
- Many people perceive quantum-safe cryptography as “not urgent,” despite the lead times required to analyse new cryptosystems and implement them in security protocols and products

Source: Mike Brown, ISARA Corporation

“When you ask managers how many clients would they would lose from a data breach, how much market share and money, it soon gets very tangible

Google’s 50 qubit quantum computer will be ready this year, the company says. IBM expects to sell commercial 50 qubit computers in the next couple of years. Both machines will be game changers.

“We are in a similar situation to the Y2K fiasco,” Mike Brown, ISARA Corporation’s chief technology officer and co-founder, told the ISACA conference. In the rush to the end of the last millennium, companies spent hundreds of millions of pounds to ensure that their computers did not stop working when the clocks turned to zero on 1 January 2000.

Y2Q – as Brown called it – could have a similar impact because quantum computers work differently to standard computers. They solve different types of problems – and are especially good at breaking codes. Given the user address for a Bitcoin, for example, a quantum computer could work out the security code that protects the money from being stolen in a couple of minutes.

The problem is not necessarily that all encrypted data will be automatically open for anyone to use – the issue today is that many organisations do not know what data relies on encryption and what does

not. If they are storing data today that needs to be safe for beyond Y2Q, that needs to be assessed soon for its ability to be safe when quantum computing becomes commercially available.

“Organisations need to do a risk management assessment of all protocols and clients, and servers need an in-depth review,” he said. “This requires coordination between vendors, OEMs and customers to catch all of the interactions.”

The data most at risk includes any encrypted data where the key to unlocking it is communicated or stored along with the data, digital documents with a long shelf life, and signed software. The most difficult part will be to secure those transactions where different systems need to talk to each other because they often rely on public encryption protocols. “Interoperability will be the killer,” he said. And while quantum encryption will probably come along, it is unlikely to be rolled out quickly enough for many organisations.

Art of war

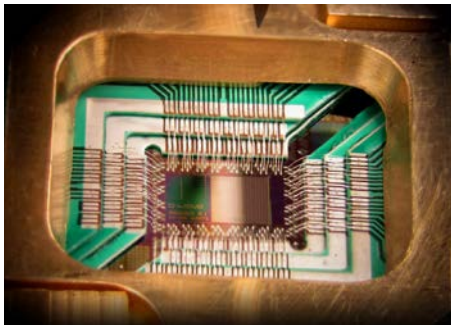
“IT security is a grave concern for a company and must be thoroughly studied,” Tom Madsen told the conference – an IT specialist who worked for the United Nations Development Programme for 12 years. He was paraphrasing the ancient Chinese strategist Sun Tzu and his classic warfare text *The Art of War*. “IT is the foundation for what we do,” he added.

He said that external threats were often not treated seriously enough from a risk perspective. Quite often, businesses patched and mended their security systems after minor incidents rather than undertaking a full forensic investigation to make sure that the attack had not uncovered a more important flaw in the organisation’s defences.

“Every time we take a decision on the system, we are changing our risk profile,” he said. “For example, are you changing the antivirus program because you have a better offer, or because you are looking for better security?”

Since all warfare is based on deception, he said, employee training on a regular basis was the key to limiting risk from cyberattack. “Whatever you do in training must

Image credit: D-Wave Systems, Inc.



Above: A chip constructed by D-Wave Systems Inc. designed to operate as a 128-qubit superconducting adiabatic quantum optimization processor.

Previous page: IBMers Sarah Sheldon and Pat Gumann working on a quantum dilution refrigerator.

be done again and again and again,” he said, “because if you do not have staff who are properly trained, or policy and procedures in place to help staff know how to act, you are leaving yourself wide open.”

Business focus

“Full business engagement is essential to provide an appropriate and sufficient protection to business’ most critical IT resources,” Paul Phillips ISACA’s Technical Research Manager said. But that was not an easy task. “This is not just about cyber security but engaging busy leaders who want to do the right thing but have other priorities outside of cyber security.”

He said that it was essential for risk managers and cyber security experts to approach the issue from a business perspective. When a breach happened, for example, executives seldom wanted to know the technical details. Instead, they focused on issues such as how much it would cost, how quickly it could be put right, and whether there were legal and reputational issues to address.

Phillips said that cyber risk should be considered as an enterprise-wide business risk – without IT systems it could not be business as usual. As well as risk professionals helping to develop a common, business-oriented language, they needed to be able to demonstrate the return on investment expressed in hard cash terms.

“We need to articulate risk by focusing on the impact – not just threat or risk – and express that in dollars,” he said. That would require risk and IT leaders to speak to people in the business and ask difficult questions. For example, how could a security breach damage reputation and stock value? “Ask them how many clients would they would lose, how much market share and money. It soon gets very tangible,” he said.

Machine learning

While people are key to an effective cyber defence strategy that ties security and business objectives together, machine learning technologies are beginning to help organisations combat hard-to-detect attacks.

Last year, for example, an international sports company



The battlefield is now inside corporate networks and it is no longer sufficient to rely on a perimeter to secure the soft interior

installed sophisticated video conferencing equipment to support its ever-growing number of overseas teams. But a hacker managed to gain control of a conferencing camera and use it to take out large volumes of data from the business’ network. Such attacks can take months to detect and the breach left the company open to corporate espionage, ransom and several other threats.

Using machine learning technologies developed by a Cambridge-based company called Darktrace, the company could detect unusual data flows from the camera. The software models a system’s behaviour from scratch with no pre-defined parameters. It builds up a picture of the network showing how data flows through the business and then analysts can dig deeper into the detail if they detect anomalies.

“The software is building up a pattern of life for the network,” says Darktrace’s Sam Alderman-Miller, “which acts as a norm against which we can detect unusual behaviour without interfering with the normal

running of the business. As the company changes, so the patterns of what constitute normal will change.”

The aim of such machine learning techniques is to develop a pattern of behaviour across the network that can be monitored in real time. The system can also wind back the time clock to see which other machines and devices the compromised network has been communicating with making it easier to trace where any lost data has gone.

The good old days of focusing all of your corporate effort in preventing a breach seem like a thing of the past. “The battlefield is now inside corporate networks and it is no longer sufficient to rely on a perimeter to secure the soft interior,” Alderman-Miller said. Companies are going to need all the tricks in the book to keep in front of developments that are right on their doorsteps. ☞



ISACA is an independent, nonprofit, global association for IT professionals: www.isaca.org. Enterprise Risk would like to thank ISACA for its hospitality in Munich.

BUSINESS DRIVEN SECURITY STRATEGY

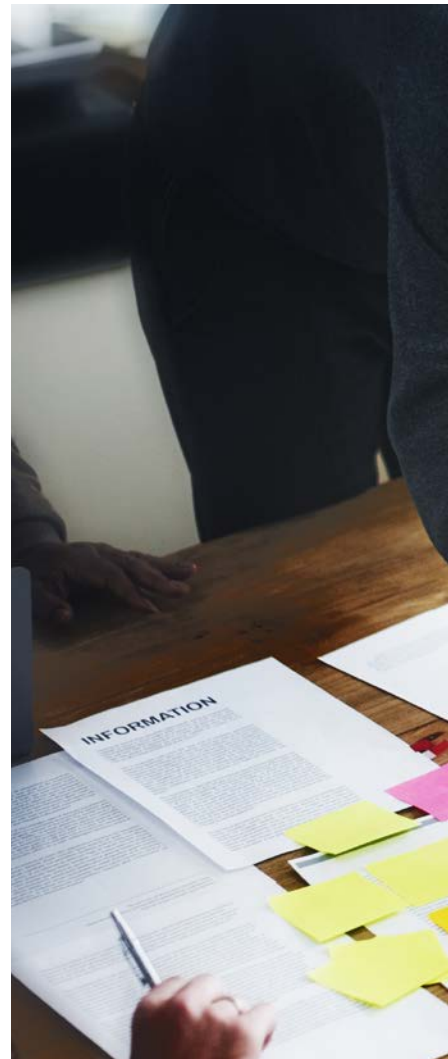
- Prioritise assets and understand their vulnerabilities
- Quantify business risk and impact if those assets were compromised; determine if your budget is allocated properly
- Build a strategy to defend those assets with clear cost/benefit relationships outlined; make sure your strategy is holistic (people, process, technology)
- Determine gaps between what you have in place today and your ideal state
- Take a phased approach to addressing the gaps, but start today; prioritise according to impact on risk posture
- Constantly re-evaluate threats and vulnerabilities to tune your strategy; have a response plan in place

Source: Paul Phillips, ISACA

Planning for success

Risk managers can make a crucial contribution to the success of new business projects

..... BY GARETH BYATT



We take and manage risk to seek reward and achieve objectives. All projects involve risk, some more so than others, but risk should be understood as meaning uncertainty, which covers both threats and opportunities. Inbuilt into every project planning process should be the creation of a project Risk Management Plan (RMP), or a subset of the project management plan, to define how the project team will take and manage risk.

An RMP should be put together by a project risk coordinator, who is appointed early in the project's life by the project manager as the project team structure is being defined. Whether the risk coordinator is a full-time or part-time role on your project depends on the project's nature and size. Many high-risk large projects employ a full-time risk manager.

Whether it is a full or part-time role, the coordinator needs to liaise with all project disciplines and be the glue ensuring that managing risk is done cohesively and collaboratively, not in functional silos. If your organisation has a central risk function, they should support the risk coordinator. They can provide guidance for the RMP and perhaps include them in any risk



The team environment and culture is a defining influence on how a project team takes and manages risk

.....



champions' network to provide mentoring and skills development.

The plan

Risk managers need to include four critical elements in the RMP. First, set out how all disciplines/teams on the project will manage risk in a coordinated and common way, focusing on achieving project objectives. Second, specify roles and responsibilities for taking and managing risk. That includes defining a governance structure to oversee this activity, including deliverables for phase and gate reviews.

Third, articulate how the management of risk will be embedded into the rhythm of everyone's activities, as part of the team's culture. And finally, describe how you will leverage your organisation's knowledge and resources, such as

central personnel, lessons learned from other teams, templates, tools and techniques.

The team environment and culture is a defining influence on how a project team takes and manages risk. It is important to ensure that people's attitudes and behaviours to risk are aligned with the objectives of the project, and that team members are clear on what is expected of them. The team's understanding of its risks must be consistent with how these risks are being communicated and discussed with the project's parent organisations and other stakeholders.

At the earliest possible time – this should be described in the RMP – the risk coordinator should assist the project leadership team in applying recognised good practices to ensure a healthy environment and culture. The IRM's practical framework for establishing and maintaining

a healthy team environment and culture is helpful here (*Risk culture, resources for practitioners* is free to members and can be found on the IRM website).

Risk appetite

A risk appetite statement is a good way to define your propensity for taking different types of risk. The use of risk appetite is common in some sectors, particularly finance. It is used sparingly in many sectors, if at all.

Defining your risk appetite for your project, and agreeing it with key stakeholders, can play a useful role in informing people where your focus needs to be. A project that needs to take risks to achieve ambitious financial objectives will have higher appetite and tolerance ranges for financial risk, for example, than a project which is financially risk averse.

Establishing and communicating a clear risk appetite fits naturally with establishing the right team environment and culture to manage risk.

Risk appetite is most effective when it is either created by the team or guided by the project's parent organisation, and then integrated into how the project team collaboratively evaluates and manages their risks across all disciplines. When risk appetite is being considered during regular reviews and daily activities, it has established itself as a valuable tool for decision-making and to measure performance against objectives – of which, more later.

When the right team environment and culture is in place, and your appetite for risk is understood, taking and managing risk should be ingrained into everyday activities. It leads to the proactive anticipation of risk and measuring the cost-benefit of actions, and having the resilience to respond in the best way possible to risk events should they occur.

Prioritisation of risk is important. Many of us are familiar with an “impact x likelihood = rating” method to prioritise risks into a “risk matrix heat map” and/or a risk register. Using a risk matrix – the levels in which will be influenced by your risk appetite – to prioritise risks, and displaying these risks in a heat map, is a good starting point. But additional factors should also be considered to improve the quality of prioritisation and focus (See box, *Priority and focus*).

Critical controls and tools

Prioritising risks helps us focus on the prioritisation of controls. Having the right controls in place to manage risks, rating control effectiveness and testing controls is a fundamental part of risk management. Controls must be proportionate to the risks that are faced so that effort is focused on what matters most. Controls rated as “critical” are those that have the largest effect on managing the risk. They are the most important controls to focus on and to have appropriate assurance in place, for example, through functional, internal and perhaps external audits.

The RMP should describe a risk toolkit, perhaps provided by your organisation's risk team, of techniques and tools that will help the team.

PRIORITY AND FOCUS

- 1. Impact:** most risks have multiple consequences; many risks are inter-related. Collaboratively review the full impact to your objective(s) if the risk were to occur by understanding all consequences and the knock-on effects of the risk to other risks and objectives. A matrix can help with this in which the rating of a risk goes up if, by occurring, it drives up the rating of other risks.
- 2. Likelihood:** use good quality data to confirm the likelihood of a risk occurring. It is also vital to understand the current controls in place for the risk and to know (through fact-based evidence and audits) how effective they are. If you have gaps in the control environment, particularly for critical controls, the likelihood of risks occurring for which they are associated with will be higher until you plug the gaps.
- 3. Appetite:** review how the project's risk appetite will be impacted if the risk occurs, for example forcing metrics out of tolerance and what that would mean to project performance.
- 4. Risk relationships:** which risks demonstrably have a large impact on other risks if they occur? You can identify this in a matrix structure.



Establishing and communicating a clear risk appetite fits naturally with establishing the right team environment and culture to manage risk

The toolkit should complement the processes already used by all disciplines on the project.

Typically, tools will include an IT risk tool, which can be anything from a shared risk register, to a comprehensive source of knowledge for all risks and controls. Most tools are likely to help teams to manage their risks, events, incidents and audits in an online, collaborative and efficient way that is better than using document versions.

But they should also include risk workshops, for example, that are planned, structured and run by a facilitator. They can be planned into the project schedule for key milestones. Discipline-specific workshops, always with a few people from outside the discipline, should be held when required.

One simple way of helping keep the project on track is to create a risk card. It is a modest but useful tool to provide to team members. It is a double-sided and laminated card –

A4 or letter size – that summarises the key points of your culture, your risk appetite, your risk prioritisation process, and how the management of risk is measured. Laminating them makes a difference. Many team members will pin them to their desks and use them in future team reviews.

Measure it

Continuously improve your performance by measuring what is working and what is not. You can measure the management of risk and not let it go unseen if you weave your measurements into people's regular activities.

There are two useful ways of measuring the management of risk. The first measures the cost of controls and actions to manage risks, and their effect on project outcomes. You can establish an accurate estimate of the cost of controls when the right people are in the room. Ask the question during



your reviews. When you monitor how well controls are contributing towards project performance, you can demonstrate their financial value, whether they are safety controls, design controls or others.

The second, is to measure the cost of managing risk against risk appetite performance and project outcomes. By using your risk appetite to guide your decisions, you can track performance against risk appetite metrics over time – such as safety metrics, financial, schedule, supply chain metrics and others. This can in turn be mapped to the success towards achieving good outcomes.


Lessons

Risk managers can play an important role in educating people in their organisation about project failure and success. Use, capture and share knowledge and lessons learned of how you have managed risk, for your own benefit, and so that others in your

organisation learn from your project's experiences. NASA, for example, turns their capture of risk knowledge into knowledge-based risks, which are freely shared and disseminated.

Your knowledge repository, structured in an appropriate way, will provide people with a valuable information source before and during their projects. Your RMP should include how you will run knowledge capture sessions, such as peer assists (seeking knowledge before activities commence), after action reviews (quick-fire learning during activities), and retrospectives (post-implementation lessons learned). Incorporating these activities into the risk management schedule will produce a rich source of information for the entire business.

Taking the time to plan, implement and monitor good practices to take and manage risk increases the likelihood of achieving project objectives. Taking the time to measure your management of risk,

and ensuring knowledge is shared, allows you to tangibly demonstrate the cost-benefit of your activities. 

 Gareth Byatt is an experienced risk practitioner based in Sydney, Australia.

 **Risk managers can play an important role in educating people in their organisation about project failure and success**

Predictably vulnerable

Why do seemingly sound organisations unexpectedly fail?

..... BY ANTHONY FITZSIMMONS & DEREK ATKINS

Why do seemingly sound companies led by intelligent, well-meaning leaders fail despite large, diligent risk management teams? We had been asking ourselves this question for years. We saw glimpses of patterns, but an important breakthrough came when we were part of the Cass Business School team that produced *Roads to ruin*, a seminal report commissioned by Airmic's John Hurrell. That project sparked a series of further collaborations that led to our book *Rethinking reputational risk* and to our conclusions in this feature.

Let's start with a hypothetical case study. A company announces that its profits have been overstated by £300m. The board is stunned, shareholders are furious and the board commissions an inquiry. A few months later, the answer emerges: the accounts team over-stated receivables.

As recently as the 1980s, it was common for an air accident investigation to conclude that the accident was caused by "pilot error". As Stanley Roscoe, a leading aviation psychologist of the time, wrote, this conclusion was "the substitution of one mystery for another". He thought aviation investigators could do much better. Subsequently, they have done so and so



Leaders are more important than they realise

.....



Left: Firemen attending the scene of a fatal airplane crash.



Boards and their equivalents have the greatest power to do good. In equal measure, that brings the power to do harm and damage

.....

should we. The best tool is the two-year-old's question: why?

Why?

.....

Going back to our hypothetical case study, we can dig deeper. Why did the accounts team overstate profits? Because they were always testing boundaries as they tried to increase profit. Why? Because they believed the CEO wanted to maintain a steady increase in profits. Why? Because they thought his self-esteem and bonus depended on steadily rising profits. Why? Because the board set his bonus that way, and his character was such that he seemed to see success in terms of ever increasing profits. Why? Because the board didn't consider risks from unintended consequences of his bonus scheme or from the character of the leader they had recruited. Why? Because the board

lacked sufficient people skills, and as a result they were oblivious to their lack – and they missed other risks stemming from human behaviour.

It is worth probing in other directions too. Why didn't the board and audit committee spot the accounting problem? Because they had an inadequate understanding of how the business made its money. Why didn't the auditors push the issue? Because the lead audit partner didn't want to risk becoming the person who lost this prestigious longstanding audit for his firm.

These questions highlight risks that appear in few risk registers, yet they are key drivers of reputational risk and damage.

Leaders matter

.....

Leaders know they are important but they are more important than they

realise. Leaders matter in proportion to their influence and power because leaders set strategy, systems and powerful drivers of behaviour beneath and around them.

At the summit, boards and their equivalents have the greatest power to do good. In equal measure, that brings the power to do harm and cause damage. This applies both to what they achieve and how they achieve it. For example, Lord John Browne did great things during his time at the helm of BP. Profits soared and its share price almost tripled at its peak.

But the Baker Report into the Texas City disaster, which killed 15 people on his watch, concluded that BP's leaders had failed to lead on process safety, something the Chemical Safety Board had concluded was a cause of the accident. Lord Browne announced his early

retirement four days before the Baker report was published. BP was left with a developing history that made it vulnerable to reputational damage in ways that appear in few risk maps.

The hole in risk analysis

A good place to start is our definition of reputational risk: *the risk of failure to fulfil the expectations of your stakeholders in terms of performance and behaviour*. Seemingly simple, this definition has great depth.

Our fundamental insight is that important risks to both the business and its reputation are not captured by classical risk management. These risks were identified in *Roads to ruin* as underlying risks. We now call these behavioural, organisational and board risks, and they are ubiquitous. They are also double-acting: they increase an organisation's vulnerability to crises by causing systemic weaknesses; and if a crisis occurs, they also help to tip it into a reputational calamity.

Going back to our definition of reputational risk, much performance risk is picked up by classical ERM. In contrast, relatively little behavioural risk – including organisational and board risk – is captured, especially at leadership levels. This is the hole in classical risk management and it matters. Risk managers are adept at managing the risks they do manage. But far too many calamities emerge through this hole, which goes a long way towards explaining both why, despite armies of risk professionals, the banking and innumerable other crises could happen – and why those crises caused so much reputational damage.

Hard to see

Risks in this group are difficult for current risk managers to find because most lack the know-how. Risk managers also need clear authority from the very top to seek out, report and deal with these risks because their root causes often lie with leaders. No risk manager can be expected to put their career at risk by analysing their superiors' behaviour, let alone through a risk lens.

These risks are difficult for any insider to see because cognitive biases prevent us from seeing ourselves

EXAMPLES OF BEHAVIOURAL, ORGANISATIONAL, BOARD AND REPUTATIONAL RISKS

- Inadequate diversity of skill, knowledge, experience and perspective among leaders
- Ineffective challenge to leaders
- A reluctance to listen to and digest unwelcome news
- Organisational complexity and internal silos and slabs (horizontal silos)
- Ignorance of how heuristics and biases affect perception and decision-making
- Complacency, failure to examine the role of luck in success and “if it ain’t broke don’t fix it”
- Groupthink
- Character weaknesses, such as a lack of courage to challenge effectively and a reluctance to listen to criticism
- Failure to set tone from top and to “walk the talk”
- Inappropriate incentives: for example the unintended consequences of bonuses; and behaviour that discourages learning from mistakes
- Communication failures
- Inability to learn systematically from mistakes
- Perceptions of corporate history
- Inadequate crisis strategy, planning and practice



Our fundamental discovery is that important risks to both the business and its reputation are not captured by classical risk management

as clearly as equally well-informed outsiders could. They are also hard to discuss because humans operate under complex social conventions including what anthropologists call “social silences”. There are subjects people will not discuss because, as the *Financial Times* journalist and anthropologist, Gillian Tett put it, they seem “dull, taboo, obvious or impolite”.

Complacency

Unseen, risks of these kinds fester and incubate, unmanaged, often for years. In the meantime, leaders understandably believe all is well. The truth is that they are sitting on a time bomb with a dodgy clock.

While leaders think all is fine and no-one questions the extent to which success is due to good luck, these systemic risks manifest regularly in small ways that are dealt with by nimble thinking

Below: The Texas City Refinery explosion occurred on March 23, 2005, when a hydrocarbon vapor cloud was ignited and violently exploded at the ISOM isomerization process unit at BP's refinery in Texas City, Texas, killing 15 workers, injuring more than 180 others and severely damaging the refinery.




people who can see the board as outsiders to the board's business and social circle. They also need the strength of character and independence to hold nothing back even if uncomfortable truths have to be explained to leaders.

Having tackled board-level risks, you can turn your attention to developing the existing risk team and systems to find and fix these risks throughout the organisation. New skills will be needed: risk leaders need to learn the rudiments of psychology, sociology and anthropology – and you might take HR professionals with those skills and teach them about risk.

Risk teams will need explicit authority from the chairman and chief executive to delve into these risks even when the trail leads to the board. To overcome those cognitive biases it is essential, at least in the first instance, to bring in trusted outsiders to help insiders to see what outsiders' eyes can see given insiders' knowledge. Here too, character and independence matter.

Biases, incentives and complacency may encourage delay today in the hope that you do not become a case study tomorrow. But since there is evidence that potentially destiny-changing events afflict large organisations on a scale of years, not decades, wise risk managers will lead their leaders towards bringing these risks under control. And for the FRC-regulated, doing so will also provide the material needed to comply with the regulator's explicit guidance on managing and reporting behavioural, organisational and reputational risks. ☞

 **Anthony Fitzsimmons and Derek Atkins** are authors of *Rethinking Reputational Risk: How to Manage the Risks that can Ruin Your Business, Your Reputation and You*. You will find case studies of BP there. IRM members can order the book with a 20% discount here: www.koganpage.com/reputational-risk using the discount code PBLRRR20.

“ Why do seemingly sound companies led by intelligent, well-meaning leaders fail despite large, diligent risk management teams?

and crisis management. These mishaps are valuable sources of intelligence that should be captured, analysed, discussed and used to find and fix vulnerabilities before they cause serious harm. Missed, ignored or covered up, these opportunities are lost.

When something blows up and turns into a reputational calamity, leaders are regularly stunned to discover that almost everyone else seems to have known what had been going on under their noses.

Finding a fix

The human race is creative, so the range of behavioural and organisational risks is almost unlimited. Some examples from this risk area can be seen on page 30 (See *Key behavioural and organisational risks*).

Bringing risk management to bear on board-level risks is the top priority

because a board's influence brings with it a board's ability to cause extensive harm when they make mistakes. It is doubly a priority because any attempt to tackle these risks below board level without visible action at the top will undermine the effort.

Any programme to deal with these risks should begin with education for the leadership team including the board. The programme should begin with private education for the chairman because their active support is crucial to all progress. One-to-one education with an acknowledged expert is a good place to start, but many will also demand a coherent written explanation they can mull over with plenty of examples from real life.

Current board evaluation is not designed to find such risks. A new process is needed that deploys new knowledge, skills and techniques. If it is to overcome well-recognised cognitive biases it must be led by

Risk Management Training

Industry-leading training courses delivered by risk experts for over 30 years

Our training courses offer you the most practical and interactive training sessions; each course is designed to have delegates actively participate during training. We base our training on topical issues, case studies and group interaction. All our training courses can be delivered as public courses or in-house, either in their current form or tailored to each organisation.

We offer CPD and accreditation.

“IRM is not just a training institution, it’s a community that shares knowledge, experience and networking opportunities which has contributed to the furthering of my career.”

**Richard Hawkins, CIRM
Business Analyst
Rimelo Consulting**

Training courses include:

- Fundamentals of Risk Management (FoRM)
- Embedding Risk Management
- Strategic Insights into Cyber Risk
- Improving Decision Making and Expert Judgement
- Practical Risk Appetite and Tolerance
- Choosing and Using Key Risk Indicators
- Risk in the Boardroom
- Risk Reporting
- Risk Culture



Email: training@theirm.org
Phone: +44 (0)20 7709 4117
or visit www.theirm.org/training



Fit for the future

To mark IRM's 30th Anniversary, Zurich Risk Engineering offered 30 free places at their two-day 2017 client conference to IRM members. Carolyn Williams reports

The conference kicked off with a few rounds of Zurich's *Supply chain game* – a great example of using gaming techniques to really understand the dynamics of supply chain risk management. With 70% of organisations apparently suffering supply chain disruptions at some time, teams competed to see who could best ensure a sustained and profitable supply of ... Swiss chocolate!

Group decisions had to be made about production, insurance purchase and other risk mitigation measures and teams then had to navigate a risk landscape of random crop failures, health inspections, cyber-attacks and fickle consumers. For more information about the game contact Nick Wildgoose, Zurich's global supply chain product leader: Nick.Wildgoose@uk.zurich.com

One area of strategic risk for many organisations arises from aging populations and the incidence of dementia. Michael Hornberger, Professor of applied dementia research at the University of East Anglia and game designer Maxwell Scott-Slade showed how innovative online game technology and big data techniques can be used to measure navigation skills and hence potentially detect signs of dementia at a much earlier stage.

On a more individual note, Michael Hoeller, head of health, fitness and wellness at the Zurich Development Centre, took delegates through a series of "brain jogging" exercises, said to build new neural pathways and improve brain health.

As a tireless fleet of robot mowers tended the lawns surrounding the development centre, delegates inside learned about the impact of technology on risk engineering, with presentations covering nanotechnology, cyber risks, safety in autonomous learning for drones, additive manufacturing (3D printing), risk perception and decision making and food safety.

IRM Honorary Fellow Stephen Carver, project risk expert and storyteller from Cranfield

University, delivered an unforgettable address on managing complexity risk. Starting from the shocking finding that 68% of change projects fail, Stephen then proceeded to explain how the aviation industry did not accept that level of failure in its "projects", much to the relief of delegates about to board planes to go home.

Zurich Insurance has been a firm supporter of IRM for many years and is the sponsor of our top student awards. The best performing students in our 2016 Certificate and Diploma examinations were given an expenses-paid trip to Zurich for them and a guest to collect their awards at the conference dinner. Congratulations to Certificate Student of the Year Alexandra Bedford and Diploma Student of the year Janie Robertshaw. 🎉



The best performing students in our 2016 Certificate and Diploma examinations were given an expenses-paid trip to Zurich for them and a guest to collect their awards at the conference dinner

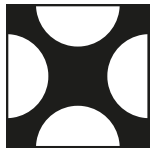


IRM chief executive Ian Livsey and IRM director Helen Hunter-Jones with Certificate student of the year Alexandra Bedford (right)



IRM chief executive Ian Livsey and IRM director Helen Hunter-Jones with Diploma student of the year Janie Robertshaw (right)

Deliver success in today's complex operating environment



4C STRATEGIES

4C Strategies is one of the world's leading providers of risk management solutions. Combining expertise with an innovative approach, our advisory services and software solutions help organisations to build, verify and track the Readiness capabilities they need to deliver on their strategic and operational objectives. Our Exonaut™ software delivers a platform from which organisations

can identify and assess risk, implement mitigation strategies, record validation activities, track real-time performance and respond dynamically to major incidents. The Exonaut™ suite of integrated modules is supported by an enterprise-wide mobile app, which enables staff to log and access critical risk data, wherever they are in the world, to support risk-informed decision-making and performance optimisation.

 **Dr Aarti Anhal Gooden**
 **+44 (0)20 3795 2350**
 **aarti.anhalgooden@4cstrategies.com**
 **www.4cstrategies.com**
 **4C Strategies**
20 St Dunstan's Hill
London
EC3R 8HL

Enterprise risk management and risk analysis software



Since 1999, riskHive have been an established global provider of professional cloud, intranet and desktop solutions for the management and analysis of RAID (risks, issues, assumptions and dependencies). Low maintenance, highly-configurable and cloud-based, the riskHive Enterprise Risk Manager application can get you online in under 24 hours, supporting your

existing processes and terminology. Easily import existing risk information to quickly produce a consolidated risk portfolio. Contact us today for your free 10-day trial of our ERM or Analytic software solutions. The ERM application, settings and data are easily transportable to your own IT infrastructure if desired.

 **Ian Baker**
 **+44 (0) 1275 542 839**
 **ian.baker@riskhive.com**
 **www.riskhive.com**
 **riskHive Software Services Ltd.**
Dilkush, Farlers End
Bristol
BS48 4PG

Leaders in Forensic Investigation



Hawkins, established in 1980, provides specialist forensic root cause analysis and expert witness services to the insurance, loss adjusting, risk management and legal professions. The company has offices in the United Kingdom, Dubai, Hong Kong and Singapore. All offices are staffed by highly experienced forensic scientists and engineers from a wide range of disciplines.

 **Graeme Drysdale**
 **+44 (0) 1223 420400**
 **enquiries@hawkins.biz**
 **www.hawkins.biz**
 **Miller House**
120 Cambridge Science Park
Milton Road, Cambridge
CB4 0FZ

Risk and audit management software solutions



Symbiant are one of the world's leading providers of Risk and Audit management software. The solution is designed for collaboration and comes as a complete suite which can be separated in to Audit or Risk sets. Symbiant is designed for non Risk / Audit specialists to use, simple and intuitive but with a lot of back end flexibility and automated functions. CIO magazine

have rated Symbiant as one of the top 20 risk solutions in the World. They have off the shelf or custom solutions to fit all budgets and requirements. Install on your own infrastructure or SaaS. 30 day free trial.





 **Andrew Birch**
 **+44 (0) 113 314 3339**
 **irm@symbiant.co.uk**
 **www.symbiant.co.uk**
 **Symbiant**
1 Whitehall Quay
Leeds, LS1 4HR
United Kingdom

Risk, insurance and safety technology solutions



Ventiv Technology is the preeminent provider of global risk, insurance, and safety technology solutions. Working in partnership with our clients to understand their challenges and key business objectives, our solutions adapt to your precise needs and evolve with you. Providing a central platform to work across your company and functions to eliminate silos and

help embed risk management. Delivered with Ventiv's extensive risk management and technology experience to provide unsurpassed client value and operational excellence. Winner of 2016 IRM Risk Management Solution of the Year.

 **Angus Rhodes**
 **+44 (0) 7808 905877**
 **angus.rhodes@ventivtech.com**
 **www.ventivtech.com**
 **Ventiv Technology**
30 Eastcheap
London
EC3M 4PL

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

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

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

Risk management software



Origami Risk is the industry's #1 Risk Management Information System (RMIS) as ranked by the 2016 RMIS Review. Founded by industry veterans committed to bringing new ideas and advanced features to the RMIS market, Origami Risk's innovative software is designed with the latest technology and a focus on performance and ease-of-use. It features powerful workflow, advanced

reporting and analysis tools, and intuitive features to improve productivity and better manage Total Cost of Risk—saving our clients time and money and enabling them to be more successful. Learn more at www.origamirisk.com.

 **Neil Scotcher**
 **+44 (0) 7775 758655**
 **nscotcher@origamirisk.com**
 **www.origamirisk.com**
 **Origami Risk**
4th Floor, Victoria House
Victoria Road
Chelmsford, CM1 1JR

Risk management software



Xactium is a cloud based Risk Management software vendor that is changing the way regulated organisations evaluate and manage their risk. Our aim is to enable risk and compliance managers to transform the value of risk management within their organisation, through the use of modern, agile and collaborative software. Our risk management platform ensures that organisations such

the FCA, Direct Line Group, HS2 and HomeServe can stay up to date and respond rapidly to both business and regulatory change.

 **Rob Stephens**
 **+44 (0) 114 2505 315**
 **rob.stephens@xactium.com**
 **www.xactium.com**
 **Xactium House**
28 Kenwood Park Road
Sheffield
S7 1NF

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 262 351**
 **ross.ellner@riskconnect.com**
 **www.riskconnect.com**
 **Riskconnect Ltd.**
11 Leadenhall Street
London
EC3V 1LP

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

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.

 **Enrico Bertagna**
 **+44 (0) 207 220 0707**
 **enrico.bertagna@awac.com**
 **www.awac.com**
 **Allied World**
19th Floor, 20 Fenchurch Street,
London, EC3M 3BY

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

Don't shoot the messenger

Whistleblowers occupy a strange place in corporate culture. They are the good guys who nobody likes

It's over fifteen years ago since Sherron Watkins, a former vice president at the US energy company Enron, became famous for blowing the whistle on corporate fraud in 2001. She made the cover of *Time* magazine for a person of the year award in 2002 for her bravery.

Her joint award winners included other whistleblowers – Coleen Rowley of the FBI, who said the agency ignored key information prior to the terror attacks on New York in 2001, and Cynthia Cooper who unearthed huge corporate fraud at the telecommunications company WorldCom in 2002.

Feted by the media for their bravery, none were employed by corporations ever again. Watkins is a speaker on faith and ethics in the workplace, and Cooper is now an inspirational speaker on workers and ethics. Rowley is a political activist.

When Mimi Swartz, who co-wrote a book on the Enron debacle with Watkins, caught up with the whistleblower-turned-speaker last year, she noticed the ghosts still followed her. Watkins revealed that she went to reunions at Enron, but that some former colleagues still avoided her. "It boggles my mind that someone still thinks I'm responsible for bringing that company down," she told Swartz.

Numerous academic studies show that effective whistleblowing procedures reduce fraud and malpractice in both government and in business. But protection for whistleblowers is still weak.

The European Union has recently consulted on whether whistleblower protection needs strengthening. Its impact report on the issue said poor backing for those who want to report wrong doing has "negative effects on compliance with rules on procurement, state aid, implementation of structural funds, environmental protection, and competition and



“ Whistleblowers help detect more fraud than corporate security, audits, rotation of personnel, fraud risk management and law enforcement combined


investment – and ultimately on the proper functioning of the internal market.”

Global studies say about 40% of all detected fraud cases are uncovered by whistleblowers: “A 2007 survey of 5,400 companies worldwide found that whistle-blowers help detect more fraud than corporate security, audits, rotation of personnel, fraud risk management and law enforcement combined.”

Surely, that finding alone should convince organisations to put in place proper whistleblowing procedures and to refrain from going on a witch hunt after the event to root out the person concerned.

Fifteen years on from those high-profile failures at some of the world's

largest organisations, it is unclear that the whistleblowers ever received their just deserts. But it is worth noting that in each instance, they had, time and again, raised their concerns internally with the right people in their organisations. They were either chastised, or ignored.

It is a vital issue for risk management. Secure and well-communicated whistleblowing procedures are a safety valve for the organisation. People can let off steam, vent legitimate concern anonymously, and give the business an opportunity to put things right before they get out of hand. Nobody likes the bearer of bad news. But shooting the messenger can only have disastrous consequences. 

A company's best asset? You

Advance your career with IRM risk management qualifications

International Certificate in Financial Services Risk Management

Directed self-study and online coaching <

Study in six-to-nine months <

Globally recognised <



Banking • Building Societies • Consultancies • Insurance • Regulators

Email: **studentqueries@theirm.org**

Phone: **+44 (0)20 7709 4125**

or visit **www.theirm.org/fsquals**

irm

Protecting your business from every possible angle

QBE is a specialist business insurer. We're big enough to make a difference, small enough to be fleet of foot. Our underwriters are empowered to make decisions that are important to you. And we don't just cover your risk. We help you manage it, meaning that you're less likely to have to make a claim in the first place.

For more information please contact
enquiries@uk.qbe.com quoting 'Risk Solutions'

Visit www.QBEeurope.com



6955CC/AUG16