Enterprise Risk

Winter 2016 / www.enterpriseriskmag.com

The official magazine of the Institute of Risk Management

Which future? risk and geo-politics / **New horizons:** IRM's 30th anniversary / **Lord Owen:** hubris syndrome / **Special report:** danger zones / **Catching the cuckoo:** insider threat / **Chain reaction:** blockchain

Africa rising: Risk management in Africa is fast becoming the focus of regulators and organisations

Arthur

RISK RECRUITMENT
EXPERTS

Achieve more with a specialist recruitment partner

From CRO to Risk Analyst, we have helped hundreds of risk professionals advance their careers.

Through professional consultation, market knowledge and expert advice we have offered solutions to people we work with.

96%

of our candidates recommend us to their peer group

If you're looking for an expert recruitment partner with a professional network within the risk market call us for a free consultation.

arthur.co.uk

+44 (0)203 5877 553

**6 Lloyds Avenue
London
EC3N 3DS**

Enterprise Risk

Winter 2016

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.

irm

MIX
Paper from responsible sources
FSC® C017177
FSC
www.fsc.org

Editorial

Happy anniversary to you

Thirty years ago, a group of friends and like-minded people got together to see if they could improve the quality of the work they did. They weren't too sure how to go about it. But they muddled through – establishing a professional body, working out how to create a set of best practices, and collaborating with academics and businesses to create meaningful examinations.

Slowly, the word spread, people joined, sat the newly-minted exams, shared their experiences at meetings, and organisations began to recognise the increased professionalism of the services they were receiving. Today, you are all members of that body – the Institute of Risk Management.

It is often easy to forget how professions get off the ground and what it takes to keep them going. While the sense of excitement and novelty, the feeling of being in at the start, can quickly fade, a spirit of openness, camaraderie and a willingness to volunteer are all key elements to their success.

> “If looking back has a purpose, it is to strengthen the sense of community and provide food for thought

In this 30th anniversary issue, we look at how risk management is professionalising across Africa. It is a new start for the profession in that continent. As you read the feature, you will see how pivotal individuals – Dorothy Maseke in Kenya, for example – have been key in taking the initiative, and connecting with other forward-looking individuals to get things going. That mirrors the experiences recounted in our anniversary retrospective *Towards new horizons*.

If looking back has a purpose, it is to strengthen the sense of community and provide food for thought going forward. To that end, IRM is marking its anniversary year with a special project – *The risk agenda in 2025*. The initiative will comprise a year-long series of reports, surveys, and special events designed to explore how the developments in risk management today are likely to impact the profession over the next several years.

Mark Boult and Clive Thompson in London, and Carolyn Williams on a recent visit to Africa, have already run successful, risk agenda in 2025 workshops for the IRM. Members were enthused, engaged and questioning. They worked together and shared their experiences, despite not knowing what the answers might be. During the breaks, they continued the discussions – keeping alive a thirty-year-old tradition that has helped put risk management on the map.

Arthur Piper
Editor

CIO Review

CIO Review Magazine has just rated the Symbiant Risk Management Solution as one of the top 20 in the world.

Symbiant was the only UK company listed.
ours is the most affordable,
So yes you can have the best for less.

Symbiant gives you the tools to work better *for Less*

5 Administrator users with Dashboards, Risk Registers, Risk Workshops, Capital Adequacy Simulations, Incident Reporting, Risk Indicators, Control Management, Self Assessments and Action Tracking
For only £400 per month with
free set up on a 30 day revolving contract.

What our Customers Say

"Having implemented Symbiant into our global business a year ago it has provided the complete solution we required to manage our risk and internal audit functions. It's a powerful tool, very user friendly and supported by a great team. It's a product I would certainly recommend!"
Simon Elliott – Internal Audit & Risk – The Innovation Group Ltd

"Unbelievably inexpensive" *Gartner, Inc.*

The Total Risk, Audit and Compliance Software solution
Symbiant is a modular solution that allows the whole workforce to collaborate on Risk, Audit and Compliance issues with prices starting at only £300.
Risk Registers, KRI, Incident Management, Audit Questionnaires, Action Tracking, Audit Planning, Control Assessments, Dashboards...

17 Years OF AWARD WINNING SOFTWARE

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

Contents

Winter 2016

10

14

18

FEATURES

REGULARS

20

25

28

30

34

Institute of Risk Management

IRM's team of experienced trainers deliver highly relevant, interactive and practical training to meet the needs of the risk profession globally

Short courses and workshops are offered at a range of levels from new starter to senior professional covering a wide variety of topics.

Tailored and bespoke training

As well as our popular public and off-the-shelf courses, we also offer effective and practical bespoke training. Tailored to your organisation's needs, we develop and deliver the right solution for you.

Our training incorporates organisation-specific case studies and creates a win-win for meeting both individual and organisational objectives. Our trainers will work closely with you to ensure the course's design, content and materials suit your needs.

"I just wanted to let you know that the CEO was extremely impressed by the course you ran. His exact words were "he loved the course as it stimulated lots of thoughts for him beyond the expected". Learning Consultant, Capital One.

Contact us: email: **training@theirm.org**
phone **+44 (0)20 7709 4117**
or visit **www.theirm.org**

irm

Building on strengths

While the IRM must continue developing the profession, we should all seek to improve our own capabilities, says incoming chair Nicola Crawford

As 2016 draws to a close and my tenure as Chairman starts, I would like to talk about my vision for the IRM going forward. Under Jose Morago the Institute has grown and developed and we have the highest number of members on record.

At our recent AGM we reported a surplus. Although we are in a strong position, we as an Institute must develop not only the strategic risk management capability of the industry but also of ourselves.

In these turbulent times of Brexit, oil price fluctuations, political uncertainty and unrest we must ensure that we are resilient and as an institute provide our members with the tools to be the same. We must be prepared for the opportunities and risks that the current macro-economic climate is providing and ensure we are more stringent in the investment we put into new products and services.

We as an Institute are committed to an investment programme which will deliver an enhanced membership experience, including a new website and Customer Relationship Management (CRM) system to ensure a smoother process and better management information to best serve our members and increase engagement.

We are growing internationally; recently we held a very successful series of roadshows and networking events in Africa – we have a strong leadership team looking after the regional groups in Kenya and South Africa and are looking to add additional groups in Ghana, Nigeria and Zimbabwe.

I also recently took part in a roundtable session with *Management today* (a publication from the Chartered Institute of Personnel and Development (CIPD) addressing key issues for the risk industry.

We can't assume that everyone knows about risk management. I've just come back from a trip to Turkey where I was talking to a business industrial group and leading a seminar on risk management. The first thing they asked me was, "Well, what is risk management and how do we use it?"

> " We must be prepared for the opportunities and risks that the current macro-economic climate is providing

This cements my vision on the priorities: developing the risk management profession via our qualifications, training and thought leadership; looking at women in risk and how we develop career pathways, examples of best practice and mentoring for future entrants into the industry; and finally, how, as an Institute, we can develop our own capabilities to ensure we are the voice of risk management – whilst providing value added for our members and the business community as a whole.

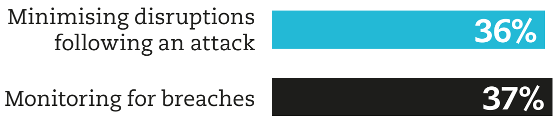
Trending

DATA

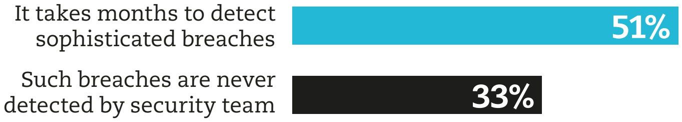
The latest stories and news affecting the wider business environment as interpreted by our infographics team

Are large companies spending budgets on the wrong cyber priorities?

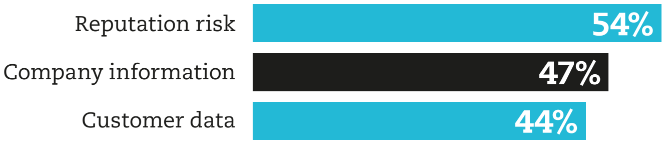
Executives that are confident of



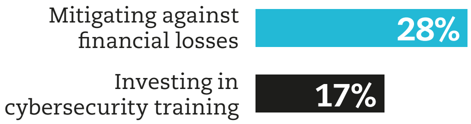
Given extra budget, most would "double down" on the same priorities, despite the fact



Companies focus on



But neglect



Source: Accenture cyber security research centre

The cost of cyber attacks

RECEIPT

Average breach cost

$665,000

Average cost of crisis services per breach

$357,000

AVERAGE INSURANCE CLAIMS

Large company

$6m

Financial services firm

$1.8m

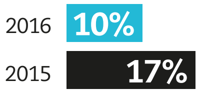
Healthcare provider

$717,000

Source: NetDiligence sixth annual claims study, 2016

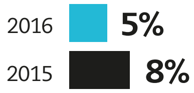
Small business feeling more exposed to cyber attacks

Fewer SMEs believe they are too small to be hacked

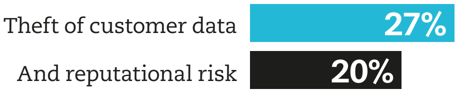


But defences weaken

(Have sufficient and up-to-date defences)



They are most worried about



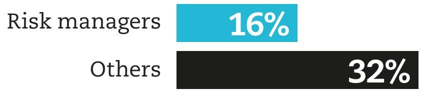
Source: Zurich Insurance Group's fourth annual global SME survey

Are risk managers out-of-sync or ahead-of-the-curve on systemic challenges?

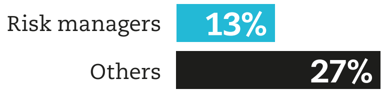
While many have been focusing on the UK's Brexit deliberations and Donald Trump's US election victory, risk managers have been more interested in other issues

RISK MANAGERS CARE LESS ABOUT

Britain's exit from the EU

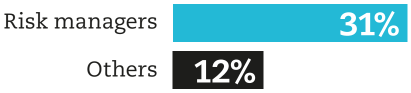


US economic slowdown

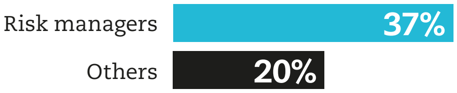


BUT CARE MORE ABOUT

The interconnectedness of risk



Sudden dislocation in financial markets



Source: DTCC, Systemic Risk Barometer, 2016, Quarter 3

Africa rising

Risk management in Africa is fast becoming the focus of regulators and organisations alike. Discover how the IRM is working across the continent to help

BY NEIL HODGE

> Regulators and governments in Africa are very keen on pushing organisations to set up risk management functions

Over the past decade countries in Sub-Saharan Africa have taken great strides to foster increased accountability and transparency in both public and private sector organisations through better corporate governance. But more recently, regulators in several African countries have also begun to seriously promote risk management as a way of improving organisational performance and resilience.

For example, Nigeria's financial services regulator has identified risk management as an essential tool to provide assurance as the country embarks on implementing the Solvency II standard, which determines how much capital insurance and reinsurance companies should hold to avoid insolvency risk.

Meanwhile, Kenya adopted a new code of corporate governance for the public sector in 2015. Called the *Mwongozo code*, it specifically states that organisations should have a risk management function and that boards needs to review the implementation of the risk management framework on a quarterly basis. It also says that boards must make a statement on risk management in the annual report, and that they have ultimate responsibility for monitoring whether risks taken are within set tolerance and appetite levels.

In March 2016, Kenya also introduced new rules aimed at improving transparency among private sector organisations. The legislation will be implemented over

> There needs to be more education to ensure that people understand that you have to build a risk culture where people understand risk appetite and risk tolerance

the course of 2017 and will require boards to disclose executive pay and how it relates to performance, and set age and term limits on directorships.

The new rules will replace guidelines that have been in place since 2002 and come after a spate of senior executives at Kenyan companies were dismissed or forced to resign over issues including mismanagement and poor performance. The country's main regulator, the Capital Markets Authority (CMA), also plans to seek powers to vet top executives (CEOs and CFOs) and members of audit committees at Kenya's 62 listed companies to strengthen accountability and shield investors from losses. It already scrutinises board members of pension funds, stockbrokers and investment banks.

Making a contribution

But it is not just regulators and governments that are championing better risk management. Those working within the profession are also beginning to shout more about the contribution that they can make to their organisations.

Early in 2016 Namibia set up a new risk management association, with the launch of the Institute of Risk Management South Africa's (IRMSA) first hub outside of South Africa. IRMSA CEO Gillian le Cordeur said the idea was borne out of a meeting she attended in the US, at which IRMSA was the only African institute represented and at which there was an obvious lack of African input. She expects to launch a similar arrangement in Botswana in 2017 and is also in talks with risk managers in Zambia.

Carolyn Williams, director of corporate relations at the IRM, says that the UK Institute is keen to develop closer ties with local risk management associations in Africa. "As a professional body, we want to work with African risk associations and help raise the profile of risk management and the benefits that the profession can add to organisations. We also want to help provide training and better knowledge-sharing. This is why we are looking to partner with more local associations in Africa."

The IRM has already set up a regional group in South Africa and, more recently, Kenya (See *Founding Kenya's regional group: Dorothy Maseke*), and it is currently developing others in Nigeria and Zimbabwe. Williams says that these groups will help develop member knowledge, as well as encourage discussion and add value to the risk profession. She also says that they will help expand the boundaries of risk management thinking, while also encouraging growth in IRM's community.

Sanjay Himatsingani, head of training and development services at the IRM, says that the Institute wants to provide help to boost the number of qualified risk managers in Africa. Currently, there are very few risk managers with professional qualifications: instead, most are from an internal or external audit background, and their view tends to be that “risk is something to be avoided”.

Accordingly, in April the IRM worked with Robert Mbonu, an IRM-qualified managing partner of Nigerian risk consultancy MCB-RMCIR, to conduct risk management and risk awareness training for 200 employees at Nigeria’s Heritage Bank. There are plans for similar training with other organisations in 2017.

Step forward

“Regulators and governments in Africa are very keen on pushing organisations to set up risk management functions, which is a great step forward for the profession,” says Himatsingani.

“However, there is less understanding about what the role involves, and not many people working in the profession have formal qualifications, which means that approaches to risk management can be haphazard and contradictory. We hope to change that that by getting more closely involved with local associations and helping them highlight the benefits that embedded enterprise risk management can bring to their organisations,” he adds.

Some countries have already taken the bold step of launching their own qualifications. In Spring 2016 the Risk Management Association of Nigeria (Riman) introduced the first formal Nigerian qualifications for risk managers. Riman designed the exams to cover international standards and local requirements. All Nigerian banks are members of Riman and the body’s executive committee has been working hard with them to encourage take-up so that all risk managers are formally qualified.

Risk managers working in Africa agree that it is the right time for the profession to capitalise on the contribution it can make to their organisations. “Risk management is certainly becoming an important topic in terms of improving corporate governance, accountability and transparency,” says Samuel Kibaara, senior risk officer at Kenya Power and Lighting Company, a public utility.

Mbonu says that awareness of

> “ Risk managers working in Africa agree that it is the right time for the profession to capitalise on the contribution it can make to their organisations

FOUNDING KENYA’S REGIONAL GROUP: DOROTHY MASEKE

Dorothy Maseke is group risk and compliance manager at ICEA LION Group, one of Kenya’s largest financial services providers. Her role includes taking care of risk and compliance activities within the group’s subsidiaries in Kenya, Uganda and Tanzania.

Maseke, a qualified member of the IRM after obtaining a higher diploma in risk management, founded the IRM’s Regional Group in Kenya in December 2015 and acts as its chair. Based in Nairobi, the group is open to members and non-members from Kenya, Uganda, Rwanda and Tanzania and aims to promote the risk management profession and facilitate information-sharing between risk professionals, regulators and corporate stakeholders so that organisations can learn from one another’s approaches.

The group holds seminars and lectures, and on 24 November held a conference that attracted over 100 risk professionals from both public and private sector organisations.

“I set up the regional group because I found Kenya had no place where risk professionals could meet regularly and exchange ideas, questions and information,” says Maseke.

“My vision is to pull together risk management professionals and encourage them to enhance their strategic influence in the institutions they work in,” says Maseke. “Through the regional group I aim to enhance risk management capacity within the region. We are excited about the growth that we have had so far, having registered ten new members over the past year,” she adds.

Maseke says that a key part of the group’s growth strategy is to establish Kenya as the centre of excellence or regional hub for risk management understanding.

The idea is progressing nicely: the group is setting up a partnership with one of Kenya’s top academic institutions, Strathmore University’s Risk Management Centre, which aims to allow students access to IRM courses, as well as provide support for their professional and academic exams. Maseke also wants to offer executive risk management training to boards of directors and senior executives.

Besides making the senior levels of organisations more risk aware and teaching them the benefits of effective enterprise risk management, Maseke also wants to use the group to help grow risk management talent from the “bottom”.

“As a way of building risk management capacity for future generations, we are currently working with members of the Greenhorn Mentorship Group, which is composed of students from the University of Nairobi. We have been speaking to them and inviting them to our events as a way to grow a pool of risk professionals,” she says.

Image credit: Carolyn Williams

Image credit: Carolyn Williams

From top left clockwise: Samuel Kibaara, Kenya Power and Lighting Company. A breakfast meeting in Zimbabwe to discuss *The risk agenda in 2025*. Robert Mbonu, MCB-RMCIR, consultancy, Nigeria. Committee members of the IRM's South Africa regional group.

risk management is growing in Nigeria and other parts of West Africa – particularly as some countries, including Nigeria, are currently in recession and so need to improve efficiency in public sector organisations. He adds too that having a risk management function is increasingly becoming a regulatory requirement (such as for financial institutions), or at least an indication of corporate governance best practice.

Taking time

However, there are also challenges ahead. Kibaara says that the perception of what risk management does is "weak". "Currently, risk understanding in most organisations – from the board to the average employee – is low. 'Risk' is still thought of as a problem that needs to be stopped, rather than as something that might provide business benefits. As a result, risk management is seen as 'risk prevention'. This needs to change and it will take time," he says.

Mbono adds that mandating that organisations must have a risk management function poses problems. "Being told that organisations must have a risk management function leads to 'box-tick' compliance. It also results in executives believing that the function assumes responsibility for risk, whereas in reality it is the job of the board," says Mbonu.

"While making risk management a priority is to be welcomed, there needs to be more education to ensure that people understand that you have to build a risk culture where people understand risk appetite and risk tolerance, and not just set up a risk management department. This is why risk training to improve people's awareness of the upside of risk is so important," he adds.

Despite the challenges ahead, risk management is firmly on the agenda in many parts of Africa. And that can only be good news for the risk management profession and for organisations they serve. ER

Neil Hodge is a freelance journalist.

Fit for which future?

Geopolitical events have radically changed what risk managers thought the future might bring. Delegates at the IRM's risk leaders' conference found out what it means for them

BY ARTHUR PIPER

"Creating a lot of risk assessments based on what's happened in the past doesn't work anymore," Richard Pryce, chief executive officer for European operations at the insurer QBE told a packed IRM Risk Leaders Conference in November. He said Brexit in the UK and the election of Donald Trump as President-elect in the US had made such an approach redundant.

"In scenario planning future high-impact events, risk managers need to understand that there is no such thing as an unlikely outcome. They should be working on the basis that a plethora of outcomes are possible," he said.

The ability for risk managers to adopt this perspective would be crucial over the next couple of years in the wake of the UK's decision to leave the European Union, he said. Pryce doubted the Government's ability to unwind the close ties with the Eurozone in the two years allotted to the process by Article 50 of the Lisbon Treaty. Scenario planning would be a crucial tool to predict the possible likely impacts on businesses of such factors as changes in currency movements, inflation rates and stock market values.

"It should be clear to everyone that we are operating in a far more unpredictable environment than we were in May this year, but it's our job to deal with the consequences of these changes on our businesses," he added.

For the insurance market, he predicted that there would be little change to the cost of insurance cover over the next

> It should be clear to everyone that we are operating in a far more unpredictable environment than we were in May this year, but it's our job to deal with the consequences of these changes on our businesses

Above: Panel discussion on risk managers' experiences of compiling the FRC's long-term viability statements. QBE's Richard Pryce, saying that risk managers needed to focus on a "plethora of outcomes" during risk planning scenarios.

couple of years, even though cross-border cover for businesses trading in multiple countries could rise a little. He saw little appetite in the industry to change the prudential regulatory framework and a need to keep equivalence with the European Union on solvency levels. Insurance premium tax was already in the hands of the UK Government, although VAT rates could be decoupled from European ones. There was real concern over keeping the so-called pass-porting arrangements, which allows for the free flow of business between the UK and Europe, he said.

Long-term viability

These political uncertainties, and the introduction of the Financial Reporting Council's (FRC) guidance to boards on producing a long-term viability statement, is likely to push risk management further up the corporate agenda. "The long-term viability statement is aimed at prompting boards to think more about risk and to avoid group-think in the boardroom," David Styles, director of corporate governance at FRC, told the conference.

The FRC was asked to develop the statements because of what Lord Sharman in his review of the financial crisis saw as a lack of quality risk reporting, a lack of integration within risk management, a lack of challenge from non-executive directors, and too much group think among board directors. He said that there was a perceived discrepancy between how businesses defined viability under the going concern rules of traditional accounting standards – usually about 12 months after the accounting period end – and how investors understood the concept of longer-term viability.

The FRC's guidance on viability reporting are part of the Stock Exchange listing rules and are mandatory, but the FRC's recent review of the first full year of reporting shows that more work needs to be done, he said. Recommending the IRM's guidance *Fit for the future?* on the issue, Styles said, "There has been a cautious, tentative approach to the first year of risk reporting, and we want to encourage a greater degree of detail in the next reporting cycle." He said most companies needed to give better explanations of the qualifications and assumptions they had made in their reports. About 75% of companies chose to report on the coming 3 years' worth of risk, he said, which tended to match forward-planning cycles.

In a lively panel discussion that followed, Helen Hunter-Jones, head of group risk at Network Rail, said it would be difficult to quantify the impact of a risk that materialised over five years into the future. Andre Katz, director, enterprise risk management, BT Group, said that the process of compiling the viability statement had helped take the business' quantification of risk up a level and it had helped him forge a closer working relationship with the finance function. "We looked at quantifying the aggregate impact of potential risk events for the first time," he said.

Seamus Gillen, director of Value Alpha, said that the longer-term impact of the FRC's viability statements would be positive. "There will be evolution in the style of disclosure, best practices will emerge, people will win reporting awards and it could create competitive advantage in the future."

irm
7th Annual
Risk Leaders Conference 2016
Future Fit - high intensity risk management for organisational longevity
Follow us on twitter
@irmglobal #riskleaders

Living process

"It's no longer possible to think in silos," General Sir Richard Shirreff, co-founder and partner of Strategia Worldwide, told the conference, "you have to look at risk comprehensively because it cuts across all parts of the business."

He said that while he had been in Iraq during the first Gulf war, when he returned in 2007, he realised that the nature of warfare had changed – and with it the risks to success. "In the first Gulf war, we knew who our friends and enemies were," he said, "but in the second, the minds of people had become the vital battleground. Similarly, the business space is more complex and it is imperative to remember that, whatever you do, you are operating among people and stakeholders are interested in what you are doing." He said that risk assessments should be considered as living projects, constantly open to change and revision.

While Sir Richard explained how military approaches to risk management could be used to develop a more holistic view of business risk (See *Enterprise risk*, Autumn 2016 *Battling risk*), Tim Johnson, chief operating officer at Regester Larkin, provided advice on crisis management – which he, said, occurred when risk management failed.

"Lack of ownership of crisis management within organisations never ceases to amaze me," he told delegates. However, he warned that the very competencies that made for a good manager could hinder effective crisis management.

"Most organisations do not make decisions quickly," he said. "In a crisis, it's the opposite. The characteristics of rapid decision making are unfamiliar to 99% of people who are in the crisis management team."

> **The long-term viability statement is aimed at prompting boards to think more about risk and to avoid group-think in the boardroom**

He said that crisis management teams needed to respond early, by putting optimism to one side and focusing on fixing the problem at hand. It was crucial to have crisis plans that are clearly written, well communicated and understood. But he said that when a crisis hits, the quality of decisive leadership was essential.

"There should be no jostling for leadership at the top because a lot of people realise they do not really want to be responsible when a real crisis hits," he said. He said each person must carry out their own role to the letter, but too often "leaders do not stay in their own lanes" and interfere with other people's priorities.

Johnson said that incident-led crises were often easy to identify, whereas those that were triggered by longer-running issues coming to a head could be more difficult to identify. To respond effectively, businesses needed to understand whether to position themselves as a victim, or as a villain. Taking the wrong stance

THE RISK AGENDA IN 2025

Risk Agenda 2025

The risk landscape and expectations on risk departments have changed beyond recognition over the past ten years. Rapid globalisation, spreading communication networks, and technological and demographic changes have added huge layers of complexity to the types of risk organisations face, and the speed at which those risks can arise.

The services and value that risk managers are expected provide to their organisations has changed too and will continue to do so into the future. The risk profession has adapted – both in the way it delivers its services and the type of work it is called on to do. Over the next year, the IRM is conducting a major project to investigate what the future of risk and risk management could look like by 2025. Engaging with members, risk leaders and key stakeholders through seminars, workshops, reports and events, the IRM hopes to develop a set of tools to help the risk community get to prepare for the future.

Workshops at the Risk leaders' conference, and in Africa, have generated enthusiasm, insight and food for thought. Please get involved and help us shape the future of risk management.

could have serious consequences for the organisation's reputation.

Finally, he said, it could be challenging to know when to signal the end of the crisis and to position the business on a more robust footing after the event. "A crisis is painful and leaders often do not want to go through what happened to share what they have learned," he said. "But the old future may no longer be possible, so the business must learn and move on in a way that is relevant to the future."

White hacker

"What most organisations don't appreciate, is that the majority of hackers are involved in running an unregulated business," Éireann Leverett, founder and chief executive officer of Concinnity Risks told the conference. That lack of understanding could have a serious impact on the way that businesses built and updated their cyber security, he said.

Leverett explained that hackers see everything in a business as a file that, once accessed, can be changed or stolen. They also were in the business of "weaponising mathematics" by analysing success rates and modifying the number and intensity of their attacks accordingly. They invested in R&D, bought attack software online and targeted common weaknesses in cyber defenses.

Active risk management was essential to keep ahead of hackers, he said. Risk managers should share data on attacks with other businesses, analyse near-miss incidents to see why they failed, shore up their defenses, target known hackers and aim to make their lives difficult.

In a breakout session, QBE's James Tuplin, portfolio manager for cyber, added that the board, risk managers and the IT team often spoke in different languages about the same issues. "Risk managers need to ensure that everyone in the business is speaking a common language on cyber risk," he said.

IRM's Risk Leaders conference took place on 24 November 2016 in London. Next year's event takes place on 23 November 2017.

irm
7th Annual
Risk Leaders Conference 20
Future Fit – high intensity risk management for organisational longevity

Top left to right: Sir Richard Shirreff of Strategia: the minds of the people are the essential battleground." Delegates. Éireann Leverett of Concinnity Risks shares white hacker insights.

Towards new horizons

The IRM is thirty years' old this year. Members past and present reflect on how far it has come and what the future could hold

"Since the inception of IRM over thirty years ago, risk management has evolved to become a core capability in helping organisations navigate the risk environment and enhance decision making," Jose Morago outgoing Chair of the IRM says. "But an increasingly complex environment and interconnected world requires a fresh approach to risk. As an Institute, our focus is now on defining the success factors of the risk management of the future."

That process is being driven by a major new project – *The risk agenda in 2025*. Over the coming year, institute members, risk leaders and stakeholders from other professions, regulators and government will be involved in a series of events to determine in what directions the risk profession is likely to travel next.

"The next 30 years will certainly be exciting for all of us," Morago says, "but the profession definitely requires foresight to understand the new set of opportunities and challenges."

Geopolitics, data and technology innovations, demographic change, developments in medicine and antibiotic resistance are just a few of the trends that could transform risk management practices. "Within this context, more than ever, risk management will be critical in preparing organisations and helping them navigate through these changes and to add value to the organisational bottom line," he says.

The IRM's 30th Anniversary is also a good time to reflect on how far the profession has come – see, *Timeline – how the profession has changed*.

irm

1986 2016 Celebrating 30 Years of Risk Management

> There was tremendous excitement when we launched the first IRM training programme and enrolled the first students

Above: A meeting of minds at an IRM course c. 1986

TIMELINE

How the profession has changed

Today – 2010s Risk management is becoming embedded within organisations. Risk officers are ensuring compliance and reporting to the executive level of organisations. Business operations are global and increasingly connected.

2000s Risk officers are appointed to facilitate risk management across the wider enterprise. They are compiling processes or implementing standards across the entire group. Business operation are becoming more global.

1990s Risk continues to be managed in silos, largely based around insurance, health and safety, or the environment. But wider elements of risk are becoming more integrated into each area. Business operations are becoming more complex as communication digitises.

1980s Risk management is handles in silos with individual responsibility for each aspect of risk. Insurance, health and safety, environmental risk are all managed separately. Operations use simpler business processes.

Beginnings

“Things were much less formal in risk management when I was involved with the IRM 30 years' ago,” Norman Bennet, says, who was involved in setting up the IRM. At the time, he was chairman of AIRMIC and so was naturally interested in exploring the further professionalisation of risk management.

“I introduced the concept of IRM to Sir Alex Jarrett at Henley Management College, who gave his support and encouragement to the idea,” he recalls. Bennett served on the IRM's Court of Governors, as the Board was known at the time. Bennett's daughter Dawn is now an active member of the IRM – currently completing her dissertation for professional qualification. “Sitting such exams is certainly a contrast to my own entry into the profession all that time ago,” he says.

“My journey with the IRM started while I was lecturing at what was to become Glasgow Caledonian University,” says Gordon Dickson, another member who was involved with the IRM in the founding days. He had been developing a degree course in risk management when he became involved with the development of the own IRM's education syllabus.

“These were heady days,” he says, “working with some great folk to build something that had never been done before. There was tremendous excitement when we launched the programme and enrolled the first students.”

He served on the IRM's Council, later as Chair for two years. Twenty-six years after becoming a professor of risk management and vice principal, he left academia and took up the post of CEO at the Medical and Dental Defence Union of Scotland.

Changing face of risk

Nyassha Asson, business development analyst (BDA) at First Citizens in Trinidad and Tobago, is an IRM student certificate member. She is thirty this year – born the year the IRM was founded. “I am a business development analyst and I started to think about careers that would allow me more scope for professional advancement,” she says. “I thought risk management may be an area that I could get into.”

Asson is involved in project management, business reporting, research, documentation of procedures, strategy formation and execution. “It's never the same thing and a lot of it depends on the time of the year or what initiatives we're currently working on,” she explains.

She saw the IRM International Certificate programme as good way of “getting my feet wet in the area of risk.” BDA is like an enterprise wide function at First Citizens and her IRM training is giving her more risk awareness and an appreciation of both the risk function's role and the responsibility the business units have in identifying, analysing, evaluating and managing risks. “Now some of the reports I do are not so much of a ‘nuisance’,” she says. “I have an appreciation for its value and thus a greater sense of responsibility for effectively aiding, as much as my role will allow, in managing risks.”

Such roles are testament to how much the IRM has achieved in helping to professionalise risk over the past thirty years. With the support of its members, it hopes to build on that success in the future. ER

Hubris syndrome

Growing evidence shows that positions of power in politics and business may corrupt the ability of those in them to behave rationally. It's time for risk managers to take heed

BY LORD DAVID OWEN

The sicknesses that heads of government have either brought to office, or developed while occupying high office, and the consequences of being ill for the business of government are a fascinating study. But, as I argue in the most recent edition of my book *In Sickness and in Power*, within this category there is another interesting and far from uncommon phenomenon to which leaders in all walks of life are susceptible. That is how the very experience of holding office seems to develop into something that causes them to behave in ways which, on the face of it at least, seem symptomatic of a change in personality.

The phenomenon of something happening to a person's mental stability when in power has been observed for centuries and the causal link between holding power and aberrant behaviour was captured by Bertrand Russell in his reference to "the intoxication of power". Power is a heady drug, which not every leader has the necessary rooted character to counteract. To do so requires a combination of common sense, humour, decency, skepticism and even cynicism that treats power for what it is – a privileged opportunity to influence, and sometimes

> **Hubris is almost an occupational hazard for leaders, for it feeds on the isolation that often builds up around such leaders**

to determine, the turn of events.

Perhaps the most profound, though non-medical, study of this was made in the ancient world. The Greeks developed the notion of hubris to characterise and explore it. The most basic meaning was simply as a description of an act: a hubristic act was one in which a powerful figure, puffed up with overweening pride and self-confidence, treated others with insolence and contempt.

Such dishonouring behaviour was strongly condemned in ancient Greece. Nemesis is the name of the goddess of retribution, and often in Greek drama the gods arrange nemesis because a hubristic act is seen as one in which the perpetrator tries to defy the reality ordained by them. The hero committing the hubristic act seeks to transgress the human condition, imagining himself to be superior and to have powers more like those of the gods. But the gods will have none of that, so it is they who destroy him. The moral is that we should beware of allowing power and success to go to our heads.

Occupational hazard

Hubris is almost an occupational hazard for leading politicians, as it is for leaders in other fields, such as the military and business, for it feeds on the isolation that often builds up around such leaders. The havoc which hubristic heads of government can wreak is usually suffered by the people in whose name they govern. The virtues of a representative democracy lie in the scope it gives elected leaders to exercise real leadership and to show the decisiveness most voters prefer to hesitation, doubt and vacillation. But the exercise of that leadership needs to carry the trust of the electorate, which is usually lost when the leader crosses the borderline between decisive and hubristic leadership. What interests me is whether that borderline, marked as yet only by loose phrases – such as “power has gone to his head”, or “she’s lost all touch with reality” – can be defined more precisely and whether philosophers, the medical profession, psychologists and anthropologists could assist in defining it.

I have been exploring the hypothesis that there is a pattern of hubristic behaviour manifest in some leaders, particularly political leaders, which could legitimately be deemed to constitute a syndrome where signs and symptoms are more often seen together than separately. I have called this hubris syndrome. Hubris is not always an easy diagnosis to recognise since the individual affected can appear completely normal in their social life. Even those in close contact with their decision-making may not pick up, in the early stages, a change of behaviour. Some psychiatrists believe that hubristic behaviour is systemic, a product of the environment in which the leader operates. On the other hand, this hubristic build-up gives the impression that it has become self-generating, that an individual is gripped by something which is no longer driven by outside factors but comes from within that individual. It is this element which comprises hubris syndrome (See *Symptoms of Hubris Syndrome*).

Hubris and risk

Having focused over the last decade on hubris in politicians, I am more concerned today about hubris in business. In the business world, the "hubris hypothesis" was first put forward by Richard Roll in 1986 in his study of corporate mergers and acquisitions, and managerial takeover behaviours. It is the most cited theory in business and management hubris research in relation to hubris-infected bidders paying too much for acquisitions.

In recent decades, risk and risk management have developed into a science. A profession with risk executives and board level risk committees has become widespread, as have regulatory requirements, particularly in the banking and insurance sectors. There have been many case studies from which one should be able to draw lessons – from WorldCom and Enron to prominent leaders of firms involved in the financial crisis (See the recent collection in *The intoxication of power,* edited by Peter Gerrard and Graham Robinson).

A study of major risk events by Cass Business School, *Roads to Ruin*, concluded that all the broad categories of "underlying risk" emanated from failings at board level and from board leadership. Better governance and an enhanced

THE SYMPTOMS OF HUBRIS SYNDROME

Proposed criteria for Hubris Syndrome and their correspondence to features of Cluster B personality disorders in DSM-IV

1.	A narcissistic propensity to see their world primarily as an arena in which they can exercise power and seek glory	**NPD.6**
2.	A predisposition to take actions which seem likely to cast them in a good light – i.e. in order to enhance their image	**NPD.1**
3.	A disproportionate concern with image and presentation	**NPD.3**
4.	A messianic manner of talking about what they are doing and a tendency to exaltation	**NPD.2**
5.	An identification of themselves with the nation, or organisation to the extent that they regard their outlook and interests as identical	**UNIQUE**
6.	A tendency to talk of themselves in the third person or using the royal 'we'	**UNIQUE**
7.	Excessive confidence in their own judgement and contempt for the advice or criticisms of others	**NPD.9**
8.	Exaggerated self-belief, bordering on a sense of omnipotence, in what they personally can achieve	**NPD.1 & 2**
9.	A belief that rather than being accountable to the mundane court of colleagues or public opinion, the court to which they answer is: History or God	**NPD.3**
10.	An unshakeable belief that in court they will be vindicated	**UNIQUE**
11.	Loss of contact with reality; often associated with progressive isolation	**APD.3 & 5**
12.	Restlessness, recklessness and impulsiveness	**UNIQUE**
13.	A tendency to allow their 'broad vision', about the moral rectitude of a proposed course, to obviate the need to consider practicality, cost or outcomes	**UNIQUE**
14.	Hubristic incompetence, where things go wrong because too much self-confidence has led the leader not to worry about the nuts and bolts of policy.	**HPD.5**

NPD = Narcissistic Personality Disorder only in DSM-IV; APD = Anti Social Personality Disorder in both DSM-IV & ICD-10; HPD = Histrionic Personality Disorder in both DSM-IV & ICD-10. Slide taken from Brain 2009: 132; 1396-1406 'Hubris Syndrome: An acquired personality disorder? A study of US President and UK Prime Minister over the last 100 years' by David Owen and Jonathan Davidson.

role for risk professionals were recommended. One of the contributing authors to this report, Anthony Fitzsimmons, traces many of the root causes to individual and collective human behavior in his recent book *Rethinking Reputational Risk*. This is most certainly an area that must be given greater attention. As recently as May 2016, Andrew Bailey, Head of the FCA, spoke of the need for improving the culture of City firms and that "hubris" should be added to the list of risks firms face.

Traits

Hubris syndrome is now perhaps better seen as an acquired personality *trait* rather than as an acquired personality *disorder*, a classification which is being more and more dispensed with. It is acquired in leaders when in power – and usually only after they have been wielding power for some time – and may well abate once power is lost. In that sense, it is a syndrome of position as much as of the person and can manifest itself at any age. The position which is held clearly affects the likelihood that a leader will succumb to it. The key external factors would seem to be these: holding substantial power, minimal constraint on the leader exercising such personal authority, and the length of time they stay in power.

Possessing self-confidence is a requirement of every executive and supports the achievement of personal and organisational objectives. It assists entrepreneurs develop their ventures, and is invariably sought after in the attributes of potential leadership candidates. However, hubris marks a turning point in which confidence exaggerates into overconfidence, pride becomes excessive and clouds rational judgement, and arrogance emerges as contempt for opposing views and contrary information. A characteristic of hubris seems to be the combined influence of these factors.

Far too often board members fail to or are unwilling to recognize danger signs in an hubristic CEO. We need to be far better at putting up boundaries against runaway leadership; improving selection, education, and evaluation by board members, and offering coaching and counseling to executives showing signs of hubris. There is also, in my view, an important role to be played by a mentor, trusted advisor or "toe-holder", which would be different from that provided by a coach. It would entail someone of independence outside the company or institution, who can help by holding up a metaphorical mirror and encourage leaders to examine their reflections with a little objectivity.

Image credit: Tilemahos Efthimiadis

ENRON
★★★★
SPLENDIDLY ORIGINAL, ENRON IMPRESSES
SLICK, HONED EXHILARATING
THEATRICAL EVENT

Above: "Enron" the play, at the Noël Coward Theatre in London's West End. The play was based on the financial scandal and collapse of Enron, the American energy corporation, based in Texas.

> "Hubris can lead to a false sense of invulnerability and to a kind of self-imprisonment

Authors of doom

In the collection *The intoxication of power*, Manfred Kets de Vries writes that hubris syndrome can lead to a false sense of invulnerability and to a kind of self-imprisonment. "The truly hubristic person ignores every opportunity for moral counsel and shared judgement," he says. "They become the authors of their own doom." All too frequently, hubris – this dangerous mix of pride, ego, delusion, resistance to criticism, and (in the case of a company or institution) groupthink – can create a culture capable of just about any mistake in the name of "we know best", he adds. Given the impact that people in the throes of hubris have on other people's lives, it is important to understand what hubris is all about.

Identifying hubristic leaders and hubristic cultures and containing them presents, therefore, an immense challenge. Such leaders are often, when first appointed, well qualified and experienced and have not given any warning signs to their electors, in the case of politicians, or boards of directors, in the case of bankers and industrialists, that they could develop hubris syndrome. By definition I do not use the term hubris syndrome where there is a known history of psychiatric illness, or of long-standing behavioural problems. Such people may be very hubristic but it seemed better to settle for their medical diagnosis, for example Bipolar Disorder, and that such a disease may all be part of a spectrum that can change and develop in power into a different personality. It is in all our interests that we learn more about such people, their hubristic cultures and develop informal systems of peer review if we are to prevent the making of damaging decisions.

In 2011, I helped to establish

Left: Investigation of WorldCom in 2002 uncovered an accounting scandal where the company's total assets had been inflated by about $11 billion. At the time it was the largest accounting fraud in history.

Image credit: ROGELIO SOLIS AP/Press Association Images

> Whilst a mass of new regulatory procedures have been put in place, as yet the role and importance of personality change is deliberately underplayed and even ignored

the charity Daedalus Trust to raise public awareness of the dangers of personality change associated with the exercise of power, whether individual hubris or collective hubris in all walks of life – business, politics and the military – and the problems that presents in terms of its effect on decision making. The Trust's work focuses on sponsoring research, holding conferences, publishing books and ensuring a high quality academic website resource, details of which can be found on the Trust's website.

Two of the Trust's advisory group members, Professor Eugene Sadler-Smith and Graham Robinson, based at the Surrey Business School, are actively working on *The hubris project* in collaboration with a wider network of senior practitioners producing proposals for three tools for the management and mitigation of hubris in business organisations. They are the first tentative steps in developing an Anti-Hubris Toolkit. They comprise the tools for empowering the board, listening to faint signals, and de-isolating and grounding the CEO – see the trust's website for more.

Hubris is an urgent problem for banking and business leaders, which they show few signs of recognising. Whilst a mass of new regulatory procedures have been put in place, as yet the role and importance of personality change is deliberately underplayed and even ignored. For all the money and time business spends on risk management, building complex models and using quantitative statistical methods, it needs to devote at least as much money and effort to biological, chemical and human resources research on personality and behaviour.

David Owen sits in the House of Lords as an independent social democrat. Under Labour Governments in the 1970s he served as Navy Minister, Health Minister and Foreign Secretary. He co-founded the SDP and was its leader from 1983-1987 and 1988-1990. He studied medicine at Cambridge and St Thomas's Hospital and was a neurological and psychiatric registrar. He has held business interests in oil, gas and pharmaceutical industries. (www.daedalustrust.com).

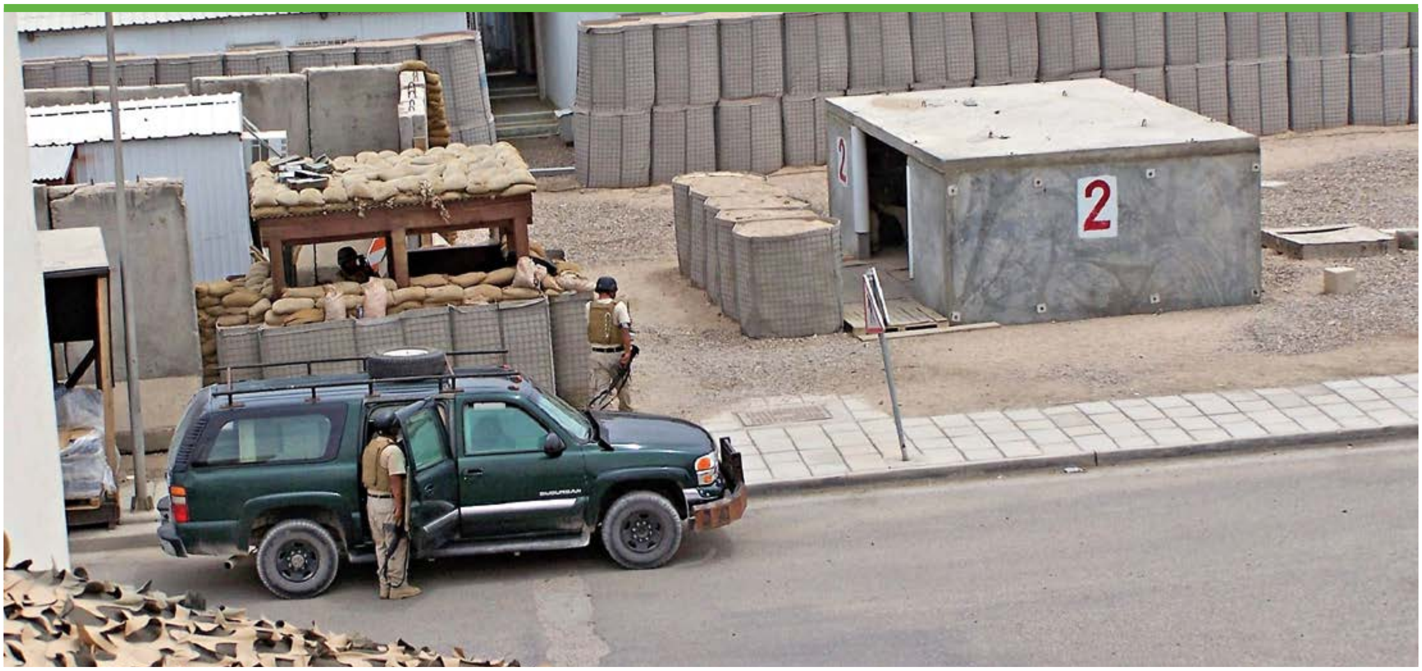


Image credit: Angela N Perryman / Shutterstock.com

Working in danger zones

With growing geopolitical instability, more organisations are sending staff into potential danger. That can pose special challenges

BY LIZ BURY

Global organisations are increasingly operating in conflict, or post-conflict zones, in disaster-hit areas, and in places affected by climate change. Whether posting staff there temporarily, or maintaining a permanent workforce on the ground, managing staff safety and ensuring the smooth running of business in dangerous places is a growing risk for many organisations.

"As the global workforce becomes more mobile, the amount of exposure that companies take on by having their staff travel around is growing," says Tim Grant, global head of security assistance at International SOS, the medical and travel security group. He says that international assignee levels have increased by 25% in the past 10 years, and the number of mobile employees continues to grow. Three- or four-year relocations, as well as short-term travel, are increasingly standard.

"There is a growing acknowledgment that organisations have a duty to ensure that individuals are looked after, and that a company's ability to remain resilient to incidents that affect their staff is crucial to ongoing operational success," he says.

Calculated risk

Risk professional and Fellow of the Institute of Risk Management Alexander Larsen, admits to taking a calculated career risk when he accepted a role as strategic and enterprise project risk manager at Lukoil in Iraq. The job involves working in shifts – 28 days on, 28 days off – managing risk at one of the world's largest oil and gas fields. The site is a two-and-a-half-hour drive from Basra airport in the south of Iraq.

"When you first come here, obviously it's quite scary." Larsen says. "Getting to site is nerve-wracking because you have a bullet-proof vest on, you're in an armoured vehicle, you've got security cars, you don't know what's happening, and you've not done it before." Once staff are in the camp, the landscape is hidden by T-walls, which are 12-foot-high, portable, steel-reinforced concrete blast walls. "What I have found is that the brain has a way of protecting you," he says, "and you forget where you are."

Since starting work in Iraq in 2014, the feeling of safety inside the company compound has been shattered only once, when earlier this year a sustained bout of machine gun fire coming from outside the perimeter walls woke everybody up at midnight. "That's when your brain starts realising again where it is, and you start panicking," he says. "Around us is marshland and sound travels. The firing sounded nearby, but it was actually at a checkpoint about 1.5 kilometres away. We don't know what happened, but it may well have been local tribes fighting each other."

Apart from that one incident, and the risks inherent in travelling to and from the airport, the main business challenges of working in Iraq have tended to reflect the fragile status of the country's nascent democratic government. The first phase of Larsen's job, when he was based in Dubai, was to establish the site. That included constructing pipelines, a gas plant, the oil processing facility, tanks for storage, well pads, and a river intake facility for water supplies. When that project was complete, the job became operational and he moved on site.

Some of the obstacles were more mundane. "When we were running the project, one of the risks that affected us most was getting visas for contractors, which caused delays," he said. "With imported equipment, there were often changes to regulations and you'd need new paperwork, and it wasn't always the most robust process — even internally, the Iraqi Government didn't always know the right procedures. And certain material isn't allowed in."

AYUDA EN LA LUCHA DE NIGERIA CONTRA EL BOKO HARAM
AYUDA EN LA LUCHA DE NIGERIA CONTRA EL BOKO
BRING BACK #OUR GIRLS
BACK GIRLS
BRING BACK #OUR GIRLS
BRING THEM HOME
DEVOLVER A NUESTRAS # CHICAS #

Image credit: rSnapshotPhotos / Shutterstock.com

"The main business challenges of working in Iraq have tended to reflect the fragile status of the country's nascent democratic government

Above: Nigerians chanting for support against Boko Haram that's claimed responsibility for abducting over 200 girls from a school in Chibok, Nigeria.

Previous page: Private security guards get out of a vehicle beside a living area protected by blast barriers and bunkers on a government camp in Southern Iraq.

Local perspectives

For example, Chinese products are perceived to have quality issues, and whether these are real or not, they can affect the sourcing of supplies to a project. In addition, the project was delayed by difficulties over land ownership with local tribes. Where the government was negotiating to buy or lease land, the business continued to feel the impact of simmering social unrest during its ongoing operations.

"The locals see this oil company and they may not be getting jobs, or they don't see the oil money trickling down," he says. If locals are unhappy, they may damage pipelines that lie outside the perimeter fence. That can cause delays of two or three days while repairs are made. "To work on it, you have to go through villages where there may be protests and everybody has guns," Larsen explains. "There is the potential for incidents whereby someone may get shot."

The lack of infrastructure — from designing and implementing effective policy, to investing in roads — continues to frustrate operations from time to time. But it is a chicken-and-egg situation. The country is still trying to establish itself. The oil facilities are important because they provide money for everything from road-building projects to social infrastructure, and more robust government. Since oil prices have plummeted, the very infrastructure that could make the work easy for Larsen's team is likely to be built slowly, or not at all.

Hot spots

Although in a very different line of work, global charitable federation Oxfam is similarly challenged by the risks of having staff work in dangerous locations. Its current top five risk hotspots for operations are South Sudan, Yemen, Syria, Afghanistan, and Somalia. It is also developing a programme in Lake Chad Basin, the area of west Africa where Nigeria, Niger and Chad intersect around a lake.

"We're scaling up there because of the humanitarian problems from the displacement caused by [the terrorist group] Boko Haram," says Heather Hughes, global security advisor, Oxfam. "That's rapidly coming up the list of countries of concern."

The risks that Oxfam staff face differ around the world, varying from relatively frequent, day-to-day type crimes, to thankfully rare but more serious incidents including kidnapping (See feature, *Taken*, pages 28-29).

"Our biggest statistic is usually crime," says Hughes. "Robbery, armed robbery, theft, or burglary, whether of our premises, people's accommodation, or on the street. In a lot of the locations where we work, our staff are relatively wealthy, so someone walking from the office back to a guesthouse carrying a laptop and a mobile phone can be a target for street robbery."

Harassment and threats pose a risk, particularly for those in frontline roles. "If you're involved in distributing something in a camp, that can get tense quite quickly," she explains. "If you're doing a distribution where everybody's getting something, that's one thing, but if it's more targeted, say for women-headed households, or for people with children, you will get people come along and say, 'Well I want this, why aren't I entitled to this?' And that can escalate."

At Plan International, a global non-governmental organisation whose focus is child welfare, Stuart Mulholland, head of global security, concurs that distribution operations can spark unrest: "If you have food shortages you are likely to have other sorts of risk, such as violence," he says. "You have to distribute food safely, and there can be community violence. It's a skilled job passing out money, and safe storage of food and provisions is very complex and can be quite risky."

Risk management

Plan International has introduced an enterprise-wide risk management system to improve the management of a whole range of risks throughout the organisation, including security risk. Oxfam also operates what Hughes describes as a robust security management framework, which supports the use of standard operating procedures for activities such as travel, compound security, managing distributions, and managing cash.

The rules can be very prescriptive for dangerous places. "In Yemen at the moment, staff are really restricted," Hughes says. "They can't walk anywhere, go anywhere after work, and they can't arrange to meet someone in a café."

At International SOS, Grant's experience is that similar jobs may have very different risk profiles and require specific combinations of mitigation depending on the location. The organisation's planning process follows a methodology based on *ISO 31000 — Risk management*, which it has further developed to include evaluation of the context of hazards or threats. The British Standards Institution and International SOS together have produced a new guidance document, *PAS 3001: 2016 Travelling for work — responsibilities of an organisation for health, safety, and security*, which came into effect on 30 September 2016.

"If you're doing an office job or a relatively standard construction job, and you put that into a remote situation where you have less available communications, or if you are working in one of the world's more austere locations, then even a standard task can become operationally difficult. Managing the consequences of a risk event needs to be planned appropriately," Grant says.

Even with the best planning, things can go wrong. But without it, organisations can be sending people into highly volatile situations with no protection. There can be no short cuts in risk management when lives are at stake. ER

Liz Bury is a freelance journalist

> **In a lot of the locations where we work, our staff are relatively wealthy, so someone walking from the office back to a guesthouse carrying a laptop and a mobile phone can be a target for street robbery**

Taken

Kidnap and ransom are top of the list when it comes to the risk of working in danger zones

BY LIZ BURY

Kidnap may be rare compared to other attacks on workers, but it has become the risk most feared by staff, particularly in conflict and post-conflict zones. In 2015, kidnapping remained the most prevalent type of violence against aid workers in Afghanistan, according to the Aid Worker Security Database, which tracks serious incidents including assault and sexual assault, shootings, kidnappings, and attacks by bombing, explosives and heavy weapons.

For humanitarian workers particularly, the context for kidnap has changed in countries where anti-Western extremists are active.

"One of the planks of our security management is 'acceptance', working with communities to make sure that they know who we are, and what assistance we're trying to bring," says Heather Hughes, global security advisor, Oxfam. "Most of our staff are local nationals, so they're often from the communities that we're working in."

She says that in terms of risk management, good relationships and a good acceptance strategy can be very helpful. "People in the community are more likely to tell Oxfam if something is going on that we should be aware of, if the context has changed, or there are some strangers in town," she adds.

Influence

However, even good local connections and support is not always enough to protect aid workers, especially because local communities tend to have less influence over the behaviour of terrorist groups such as Al-Qaeda or ISIS,

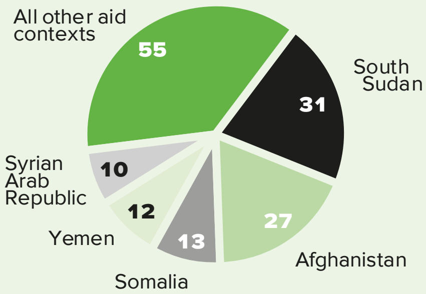
> "You reach a stage where there is no point having people in lockdown if they can't do anything

ATTACKS ON AID WORKERS IN 2015

109	Killed
110	Wounded
68	Kidnapped

Source: Aid Worker Security Report 2016

ATTACKS BY REGION IN 2015



Source: *Aid Worker Security Report 2016*

> The context for kidnap particularly has shifted in places where groups driven by anti-western ideology operate

than they may have wielded over militia groups involved in conflicts in past decades.

"I have worked in international development for 35 years, and was involved in programmes in the field in Kenya," says Stuart Mulholland, head of global security, at Plan International.

"We used to see ourselves as having special rights, but the landscape has changed since 9/11.There has been a fundamental shift where we don't have immunity from these challenges, and aid workers are targeted,"

The challenge for security and risk managers at aid agencies is to know when the balance between risks to staff and wanting to get help to people is tipping into the danger zone, and having procedures in place to protect workers.

One option if risks are escalating is to evacuate. "We do everything we can to stop kidnap from happening, and we provide staff with training about how to react if a situation does occur," says Alexander Larsen, project risk manager, Lukoil. "Where there has been escalating protest or violence, we have evacuated the site, and sent everybody to Dubai for a few days until things calmed down."

Oxfam evacuated 29 staff out of Juba, the capital city of South Sudan, in July 2016, following a weekend when a spike of fighting erupted on Friday, and was still continuing on the Tuesday.

Intense

"It was very intense and we went into what we call hibernation," says Hughes. She says that is often a first response if there is fighting on the streets. But after four days, things were not looking any better. "You reach a stage where there is no point having people in lockdown if they can't do anything, and it was very unclear about what was going to happen next," she explains. "Initially the airport was closed and then it reopened briefly, and there were a couple of opportunities, so we paid for a charter flight to get the international staff out from Juba to Nairobi."

Another group of aid workers who were unable to escape were attacked in a serious sexual assault, an incident that shocked the international aid community. Attacks related to the ethnically-driven conflict in South Sudan saw it listed as the most dangerous location worldwide in the *Aid worker security database 2016* report.

The context for kidnap particularly has shifted in places where groups driven by anti-Western ideology operate. "Although it may start off as an entirely criminal endeavour just to get some money, people may get sold to more extremist groups — that's the fear," Hughes says. She says there are many interests to juggle – not just organisational priorities – such as those of the families involved or the government. That can make kidnap situations extremely difficult to manage.

"We have a policy that we don't pay ransoms or make concessions," Hughes says. "The British Government doesn't pay ransoms either."

Oxfam has recently conducted a wide-ranging review of its crisis management plan. That has involved training for senior staff who might be involved at a leadership level in managing kidnap situations. As the risk landscape continues to change, organisations are working hard to keep their knowledge and procedures up to date and relevant.

Liz Bury is a freelance journalist

Catching the cuckoo

While many organisations have good risk management systems for detecting threats from outside, fewer are prepared to deal with the actions of malicious insiders

BY RYAN MEEKS

> The malicious insider is like a cuckoo's egg in the midst of the organisation's nest

Imagine you are an IT technician within a large corporate organisation, tasked with conducting a routine audit of the company's key servers. As you start sifting through, you begin to notice anomalies, strange indicators and unusual activity. You realise that the system is infected with a logic bomb that has been deleting key files and sending sensitive information through backdoor accounts for months. The scale and complexity of the attack is not immediately apparent, but the implications to the organisation are potentially crippling.

How did it get there? How did it go unnoticed for so long? Who did it? While it may not be immediately clear, you soon realise that such an intricate and obscured attack was not perpetrated from the outside, but originates from a much more concealed and intelligent adversary: the malicious insider – a cuckoo's egg in the midst of the organisation's nest.

Insider threats are defined as attacks to an organisation from the people within it. These could be permanent or temporary employees, or even part of the supply chain, but generally have access to the organisation's critical systems, assets and information. Contrary to common belief, malicious insiders do not typically enter an organisation with harmful intentions, but are subject

> Contrary to common belief, malicious insiders do not typically enter an organisation with harmful intentions

to an array of influences (internal and external) once inside, that build resentment, elicit intention, or even trigger a malicious act. Whatever type of attack the insider chooses to conduct – fraud, sabotage, information theft or espionage – their deep knowledge and awarded privileges allow them to exploit known weaknesses and operate under the radar for longer periods of time or, indeed, indefinitely.

Not just analytics

Insider threat is currently severely under-appreciated in risk, security and safety management circles, with a lack of the methods and understanding needed to empower practitioners with usable tools that can define, identify and mitigate insider threat. This must change in a modern world that is progressively exposing the weak underbelly of ill-prepared organisations.

The insider threat management industry has grown in recent years, with a number of vendors offering clever technological solutions. Many of these are User Behaviour Analytics (UBA) software tools, which track, collect and assess raw user data on the network, to identify malicious patterns. While undeniably useful, and an integral part of a holistic approach, many organisations make the mistake of over-relying on technological solutions to solve what is essentially a human-focussed problem.

Maybe it is fear of the unknown, or a hesitation to be seen to be turning the spotlight inwards, but over-reliance on technology is particularly common within larger organisations. Indeed, the challenge facing these organisations is sheer scale: hundreds or thousands of

KEY FACTORS IN INSIDER RISK

1. **The people** – know the nature of the workforce. Who are they? What do they do? What makes them tick?
2. **The influences** – know what the workforce may be susceptible to, both inside and outside the organisation
3. **The triggers** – know the catalysts and situations that the organisation may find itself in that could escalate the insider threat risk.

SEVEN STEPS TO INSIDER THREAT STRATEGY

The following seven steps should be considered in the development of an insider threat strategy:

1. **Gain leadership support.** Without support from the highest level of the organisation the programme will not have the required levels of reach, exposure and access to be successful.
2. **Conduct an insider threat audit.** Conduct up-front analysis to understand the people, the environment, vulnerabilities and existing controls. Envisage typical insider threat scenarios, and evaluate how the organisation could respond to and recover from a real incident.
3. **Create an insider threat management team.** Engage people across the workforce and create a dedicated cell for dealing with the issue.
4. **Implement technology.** Tools such as UBA software can be effective as an integral part of a holistic insider threat strategy. Identify what technologies are suitable and ensure that they are implemented, configured and used intelligently.
5. **Policy and process.** The strategy must be underpinned by policy and process that encourages good practice and protects vulnerabilities.
6. **Communicate with people.** Contrary to common belief, a transparent insider threat strategy that engages the workforce – for example, through training and awareness – is much more likely to be successful. Insider threat management does not have to operate in the shadows. People are the most advanced sensors and often spot suspicious indicators well before anything else, forming the most effective first line of defence.
7. **Don't forget trusted business partners.** A malicious insider may not necessarily reside within the organisation's inner circle, but may conduct an attack through its business partners or supply chain. Ensure that whatever controls are in place internally are at least matched by those in the network. Partners and suppliers provide a backdoor for insiders, so these scenarios must not be overlooked.

network users present a literal needle in a haystack scenario. This requires a more intelligent approach than a blanket technological rollout.

The algorithms on which UBA tools are based are not advanced enough to spot genuine maliciousness with 100% reliability. Questions remain as to these tools' validity, and whether they will ever be able to appreciate the myriad of complex socio-cultural, psychological and behavioural insider threat influences. Their lack of contextual intelligence often results in masses of information being delivered to the end user, and subsequent big data interpretation challenges. Technology must be implemented based on an informed understanding of the most complex, unreliable and uncertain component to insider threat: the human.

Organisations must start by attempting to understand the type and level of threat to which they are vulnerable. This is directly influenced by the organisational culture, role and job design, the nature of the workforce, type of operations and IT infrastructure. There are also wider external cultural, domestic and societal influences but these are more difficult to define. Perhaps the challenging intricacies of insider threat psychology and behaviour are the reason why so many organisations are slow in recognising the malicious insider as a viable threat. Industry must address this capability gap, as successful insider threat management relies on an understanding of the complex human factors.

Challenges

Any solution to insider threat must address five main challenges: scale, thresholds, evidence, reliability and action.

First, scale: how insider threat mitigation is addressed is dependent on the organisation's size. An SME may gain an appreciation of the threat across the whole of its operations, while a vast corporation needs to focus on key subset areas. The approach must be suitable for the number of people in which the threat could reside. Second, insiders do not want to be caught. Their knowledge of how this might happen can allow them to operate undetected. How tolerance and identification thresholds are set in relation to critical assets is important. There is a delicate balance between ensuring that thresholds enable the identification of genuine malicious actions, while limiting the unprotected dark corners that might be exploited.

Third, insider threats are rarely defined by one-off or spurious actions. The key evidence for genuine maliciousness is likely to be found in a pattern of related behaviour, with

> “ **Technology must be implemented based on an informed understanding of the most complex, unreliable and uncertain component to insider threat: the human**

the foundations of an attack in place days, weeks, months or even years before it is conducted. The success of a control, and the ability to collate evidence, is dependent on identifying these patterns as early as possible. Fourth, there is an inherent challenge associated with human behaviour. Just because a person exhibits signs that could be categorised as malicious, does not necessarily mean that they are. People are naturally changeable, non-linear and irrational, thus having absolute confidence in the reliability of findings is a major challenge.

Finally, action: if an effective system is able to identify genuine patterns of malicious behaviour and to record a body of evidence, there still remains the challenge of acting upon it. Legal considerations must be taken into account if prosecution is considered. The best strategy is to escalate the issue within the organisation once the insider threat management system has gone as far as it can go.

> The challenging intricacies of insider threat psychology and behaviour are the reason why so many organisations are slow in recognising the malicious insider as a viable threat

Strategy

If an organisation already has an insider threat strategy, can it be sure it is working? If it does not have a strategy, it should seriously consider implementing one. How this works will ultimately be dependent on the risk appetite, the nature of the critical assets, and the type and level of insider threat risk facing the organisation (See *Key factors in insider risk*).

Understanding these key areas will allow an organisation to implement a dynamic insider threat strategy that is scalable depending on the commensurate threat (See, *Seven steps to insider threat strategy*). A happy workforce, however, is highly unlikely to engage in malicious acts. If a positive and rewarding environment is created then the perceptions, motivations and behaviours that lead to insider threat acts are likely to be controlled. The focus should be on the source, instead of the irreversible downstream consequences.

Put yourself back in the shoes of the IT technician conducting the server audit who finds the logic bomb. Could that scenario still happen if all of the strategic control measures were in place? Yes, it could. However, the chances are that you will catch it earlier, you will be able to identify the source, can escalate it quickly and can collate the evidence. Organisations will never be entirely free of insider threat risk: the only way to achieve that is to not employ any people at all.

While insider threat is unlikely to be the biggest threat to an organisation's security, it is large enough to warrant a higher degree of consideration. To guard against becoming the victim of a concealed, intelligent and dangerous internal adversary, organisations today must wake up to the malicious insider as a critical threat and banish the cuckoo's egg from the nest.

Ryan Meeks is a Chartered Human Factors specialist and insider threat expert working as a consultant at Frazer-Nash Consultancy in Bristol (www.fnc.co.uk). Ryan leads the company's insider threat capability, which offers a number of analysis services to the defence, security, banking and financial services industries.

Chain reaction

The potential for blockchain technologies to disrupt the financial services industry is growing, but businesses should not rush in blindly

BY SEBASTIAN RATH

> Risk managers have a critical role to play in assessing both the internal and external risk factors that blockchain creates

The digitally-connected consumer age for financial services is here and accelerating fast. Global consumption is increasingly digitally empowered. This trend determines which financial services succeed and grow, which ones specialise, and which ones might not connect with future customers.

Digital ecosystems are success factors enabling financial services firms to thrive, to deliver superior customer-centric experiences, and to respond to increasing demand for instant analytical information. Globally, this is evident in trends for deeper business intelligence, the use of data mining, big data, and data analytics.

These developments are not entirely new, but emphasis on data infrastructures has gained significant momentum with blockchain technologies entering the mainstream. In summer 2016, the World Economic Forum said that blockchain would "become the beating heart of the global financial system." The technology promises to create an ecosystem of banks, insurers, capital market makers, brokers, governments, asset managers and pension providers that can deliver seamless customer service. But what is blockchain and why does it matter?

Unique characteristics

The origins of blockchain arose with Bitcoin, which was a response by cryptographers to systemic trust-issues

emerging from the last financial crisis. In simple terms, blockchain is just another distributed database. It comprises a list of ordered records called blocks. Each block contains a timestamp and a link to a previous block. That structure gives it five unique characteristics.

First, users write to the blockchain, but cannot delete individual blocks, which means that blockchain preserves transactional records, without deleting them. Second, unlike traditional central-ledger databases, blockchains use multiple, decentralised instances that are all-time fully synchronised. This means that users can work on multiple instances of your blockchain across the globe. While this makes the database more power hungry, it provides redundancy and data security.

Third, blockchains can automatically interact with your core data. So-called smart contract and side chains are codes that allow for effective, instant and cost-effective self-execution and self-validation of data and transactions. For example, they can facilitate payments and contractual arrangements as soon as defined conditions are met. Such automation is an inherent benefit of blockchains for customers of financial services, facilitating faster, data-driven and cost effective transactions.

Fourth blockchain's privacy can be tailored. Bitcoin introduced the concept of a public blockchain, where data is transparent and visible to anyone with access to the global public Bitcoin blockchain. But it does not have to be that way and private and semi-private blockchains require managed access and usage restrictions.

Finally, saving data to a blockchain creates data blocks that are cryptographically safe. In simple terms, hashing produces data blocks, together with a string of information uniquely summarising the block's content. Blocks are then connected to blockchains using these information strings as explicit, unique references to their prior and following blocks. This ensures that attempts to modify the block's content automatically invalidates the referencing across the chain, which fundamentally strengthens blockchain's data integrity from its beginning – the so-called genesis-block.

Big business

The funding of 92 blockchain and bitcoin startups attracted US$429m in the first nine months of 2016. Projected spend on blockchain projects for 2017 exceeds US$1bn. Banks lead in these developments, but insurers are also active. For example, the French group AXA, with its internal capital venture fund AXA Strategic Ventures made one of the largest commitments in 2016 when it acquired Blockstream. The Canadian company specialises in developing smart contracts.

Aimed at consumers, insurance startup Trov launched on-demand insurance for short and bespoke time-periods, at the click of an app, greatly leveraging the transactional simplicity of registering live contract-updates on the blockchain. During 2016, the InsurTech sector concluded that blockchain ecosystems support product innovation across the claims process, travel insurance, rental car insurance, pay-as-you-stay, home insurance, crop insurance, health insurance and patient record management. Further insurance product segments may come into focus as connected devices and the integration of the internet-of-things develop. The World Economic Forum's report *The future of financial infrastructure* provides a detailed segmental analysis of the opportunities in these areas.

High-paced risk

Blockchain ecosystems are likely to see a high-pace of development over the next few years. The key risks for blockchain is in the IT risk domain, which can be managed in a similar way to developing ecosystems in the open source domain.

Forums have established analysing and discussing incidents and technology issues in the use of digital assets, digital risk transfers and the use of blockchains in financial services. The uses of smart contracts for financial services are particularly likely to advance quickly, driven by global consortiums and blockchain providers.

DEVELOPMENTS FOR 2017

Financial services firms are likely to marry some of their existing challenges with the potential of blockchain. Four areas are likely to advance considerably in 2017 include:

- **Automating financial risk transfers**
  Applications will develop across financial and risk trading, hedging, distribution, brokerage and intermediation. Those will leverage costs, speed or operational efficiency gains. Likewise, product solutions will be blockchain-enabled. Applications across payments and claims management provide benefits for customers and firms. Businesses and their supply-chain management will be active in increasing transparency for more effective risk transfers. Some initiatives will focus on establishing deeper trust, others on connecting with new customer groups.
- **Market issues, fraud and trust**
  Since firms compete, areas for data sharing are sensitive and limited. Such competitive limitations reduce in areas where overcoming joint hurdles is important. For example, blockchain initiatives tackling fraud risk or financial abuse will credibly leverage trust and support complex, timely needs for information across participants. Such initiatives promise to credibly reduce potentially unfair costs to customers.
- **Managing climate change risks**
  For businesses, corporates and financial markets, timely access to global climate information is becoming more important. Blockchain's decentralised systems can uniquely service such needs both locally and globally. Providing immutable ledgers with permissioned smart-contracts, blockchains can enable more automated verification techniques and the use of climate statistics, leading to more dynamic data interpretation. This should facilitate actionable insights and provide the potential to deliver key indicators informing supply chains and future financial risk transfers.
- **Digital government, social and health services**
  Financial services will interact with those sectors requiring frequent data exchanges, while facing huge potential for reducing complexities, replacing aging ledger systems and exchanging sensitive information. The UK is exploring new ways of paying government benefits. Likewise, many firms have built new models tracking and completing digital heath-records, ensuring better interoperability across health services, pharmaceutical and health technology providers.

Operational key risks include scenarios of instability, impairment, disruption, maintenance, updating, future proofing and cost-control. Regulatory risks still remain largely undefined, while selected and initial views start to shape. This is often compensated by a consultative approach by leading global financial regulators, seeking discussions with industry. Likewise, legal and compliance risks for blockchain ecosystems are not mature. Together, these effects could result in reputational and financial risks, if not appropriately mitigated.

Organisations looking to adopt blockchains would do well to follow some basic steps. To get started, they should assess the skills, training needs, and organisational readiness for sandbox deployments – those that are conducted under controlled circumstances. There must be a clear reason for using the technology and the inherent value for blockchain transactions should be calculated.

Across counterparties, businesses need to establish requirements, individual expectations for leveraging blockchain benefits, a joint view for the operating model, and estimates on transaction data volumes and frequencies. They should choose a blockchain provider with clear requirements on operational, IT maintenance, costings, and inherent risks. Finally, for the overall project, establish a blockchain roadmap, with shared views on timelines, feasibility, testing, rollout, regulatory interaction and external partnerships.

Challenges

Businesses should try not to get carried away about disrupting the industry, or the buzz around blockchain technology. What matters is making a solid start. Initially, getting to a sufficiently broad understanding of blockchain across relevant parts of the firm is key because without it, it could be difficult to get buy-in. Reaching a sound commitment to fund blockchain projects can be a long journey, depending on a firm's opportunistic agility to exploit new technologies. The industry may be fast moving, but the business may need to go at its own pace.

Typically a process of thought-generation requires several iterations by dedicated teams. At early stages, potential requirements may change frequently – and the teams should be ready for this. Eventually, this leads to a maturing organisational readiness to work with external blockchain providers. Strong leadership and vision are required, together with a collaborative approach, a culture of effective innovation with focus on actions and goal-oriented outcomes. Finally, a sound grasp on the choices made helps the team to steer the project effectively given the fast-developing nature of blockchain ecosystems.

Blockchain does pose a threat to businesses that do not adapt quickly enough. But that does not mean that organisations should rush in without following careful analysis and testing programmes. Risk managers have a critical role to play in assessing both the internal and external risk factors that blockchain creates. Beyond the hype, there are likely to be real benefits for those who proceed with care.

Dr. Sebastian Rath is Principal Insurance Risk Officer at NN Group and owner of the Insurance-blockchain-forum. The opinions expressed in this article are the author's own and do not reflect the view of the NN Group.

IRM SUPPORT FOR VIABILITY STATEMENTS

IRM recently published a ten-step template as part of its analysis of a sample of longer-term viability statements – including recommendations on how listed companies should structure their longer-term viability statements.

The requirement to confirm that the company is a "going concern" has been in place for some time. But listed companies are now (since September 2014) also required to confirm that they have assessed their prospects further into the future.

This requirement to report on future prospects is embedded in the obligation to produce a "longer-term viability statement". Usually, this statement covers at least the next three years and sometimes longer. The full report can be found on our website. IRM also offers a one-day course on longer-term viability statements, which can be offered as a short course or in-house.

https://www.theirm.org/training/all-courses/longer-term-viability-statements.aspx

irm

RISK SNAPSHOT

Fit for the future?

Analysis of the scope, structure and content of a sample of longer-term viability statements published in 2016

BEST INTERNATIONAL CERTIFICATE STUDENT

IRM and the Federation of Asian Pacific and African Risk Management Organisations (FAPARMO) recently awarded Carla Knight, IRMCert, risk specialist, Exxaro, Johannesburg, with the award for Best International Certificate Student of the Year. The award was made during the South Africa Regional Group meeting on: *The risk agenda in 2025* and *Virtual-reality mining and risk*.

The best student is the individual who achieved the highest marks in the combined papers of the *IRM's International Certificate in Enterprise Risk Management* in one year and is a permanent resident of Asia, Australia or Africa.

Carla said: "I am delighted to have been presented with this award. The IRM qualifications provide you with the correct foundations that are necessary to be a successful risk specialist/manager."

CONDUCT RISK

Raza Sadiq, the Chairman of the Banking and financial services special interest group (BFS-SIG), recently welcomed a 60-strong audience to the newly-opened UCL School of Management campus in Canary Wharf to take stock of conduct risk and culture initiatives.

They were joined by a panel of experts, including Jane Walshe (Barrister and Fellow at CISI and Co-Founder of Enforcd), Duncan Wardley (Director at PwC – Centre of Excellence), and Nick Talbot (Head of Risk Standards and Frameworks at the Royal Bank of Scotland).

Nicola Crawford (Chair, IRM) and Dr Alan Parkinson (UCL Deputy Director) opened the event, introducing the audience to the IRM and to the UCL School of Management Finance curriculum and history. Nicola stressed the importance of increasing risk management awareness and ensuring a healthy dialogue on current and emerging trends in our industry – a need that the special interest group will continue to address through its series of events.

A full write up can be found on LinkedIn, search *IRM ERM in Banking and Financial Services SIG.*

CHARITY SELECT COMMITTEE

IRM's Charity special interest group responded to the House of Lords Select Committee's inquiry into charity sector sustainability. It argued that risk management should not be solely considered a health and safety issue, but needed to be central to each charity's strategic planning. "Members of the SIG helped to draft a comprehensive response on behalf of the IRM, which we hope will help the Committee understand how critical risk management is to improving the sector's capability," says Alyson Pepperill, the group's chair.

RISK IN THE NUCLEAR INDUSTRY

The 8th annual conference for the Nuclear Industry's Risk Management Association was held on the 15th November in Kendal, Cumbria. The event was well attended, with over 30 people representing the organisations that make up the Nuclear estate (JNS, NDA, Sellafield, Magnox, LLWR and NuGen).

Directory

SERVICES

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

riskHive Software Solutions

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

Insurance claims handling and risk management software

JCAD

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

👤 **Phil Walden**

☎ **+44 (0) 1730 712020**

✉ **phil@jcad.co.uk**

🌐 **www.jcad.co.uk**

📍 **JC Applications Development**
Manor Barn, Hawkley Rd
Hawkley, Liss, Hampshire
GU33 6JS

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

Risk and audit management software solutions

Symbiant®
Better Software for Risk and Audit

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

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
NTT DATA Figtree 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

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

Risk management technology

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

👤 Ross Ellner, Director, EMEA

☎ +44 (0) 7714 262351

✉ ross.ellner@riskonnect.com

🌐 www.riskonnect.com

📍 Riskonnect Ltd.
52 Kingsway Place
Clerkenwell
EC1R 0LU

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

The generation game

In four years' time, half of the global workforce will comprise Millennials. Are businesses ready for the cultural revolution this onslaught will bring?

For those of a nervous disposition, 2020 is going to be a worrying time. By then, over half of the planet's workforce is likely to comprise Millennials – those difficult-to-understand under 35-year olds who are out to change the world. They will come swanking into businesses, sweeping away hierarchies, received wisdom and set working patterns like a pack of marauding lap-top toting, mobile-addicted barbarians.

There has been plenty written about this bunch of attention-span-challenged youngsters, but recent research suggests that understanding their values could help businesses prosper.

In *Busting the millennial myth*, Peter Lewis and Ruth Yeoman say Millennials are more likely to be in precarious employment than older members of the workforce; face a harder time in securing a mortgage; and struggle with meeting higher costs of living with their less-secure incomes. On the other hand, they seek greater meaning from the work they are prepared to commit to and, the authors say, "what sets them apart is their ability to refuse requests that breach their values, their willingness to change direction and their desire to avoid 'corporatisation'".

Lewis and Yeoman argue that Millennials are best suited to working in employee-owned enterprises, but there are lessons for all in the report.

Most people want their work to be meaningful, of course, but Millennials bring with them values they have undoubtedly picked up from the ethics of the internet. That can be most obviously seen in three areas: profit-sharing, customer service, and ways of working.

Image credit: Marco Verch

> They expect work to resemble the hours they have spent with friends on Facebook, on networked games such as Counter Strike Global Offensive (CS:GO), and in building shared, virtual worlds on Minecraft

Millennials are intensely collaborative. They see business life as a team endeavour. They expect work to resemble the hours they have spent with friends on Facebook, on networked games such as Counter Strike Global Offensive (CS:GO), and in building shared, virtual worlds on Minecraft. Each person should get recognition and pay based on what they have contributed – making profit sharing attractive.

They care less about traditional ideas of customer care. That concept sounds too hierarchical to them. For Millennials, the customer is part of the broader team – the solution to customer needs based on open communication, collaborative partnership and sharing. Business is something that resembles a virtual community where everyone should benefit – not just customers and shareholders.

Finally, they dislike autocrats, or jobs where they feel there is no personal fulfilment or career progression. According to Lewis and Yeoman, their approach to business is more likely to be focused on outcomes, distrustful of meetings, and oriented to solving problems through online research and sharing ideas online. That does not mean they are just interested in doing their own thing, as some have suggested, but in doing the things that are important to the business in their own ways.

Businesses looking to benefit from the Millennial mindset need to see the whole person when designing job specifications, working methods and incentive schemes. Traditionalists will need to loosen up a bit. Provide younger people in the workforce with appropriate mentoring and flexible working methods. They will need to trust them to do the job without being micro-managed or dragged into endless meetings.

Preparing for the Millennial invasion will be about creating the right sort of open, collaborative and respectful culture. Defining and creating value for all will be key. If that sounds like the end of the world, it is time to ask why.

Institute of Risk Management

Get the Recognition You Deserve

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

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

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

What's in it for you?

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

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

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

Compulsory from 1st July 2016.

Contact IRM for further details or visit:
www.theirm.org/membership/continuing-professional-development

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

Made possible

QBE