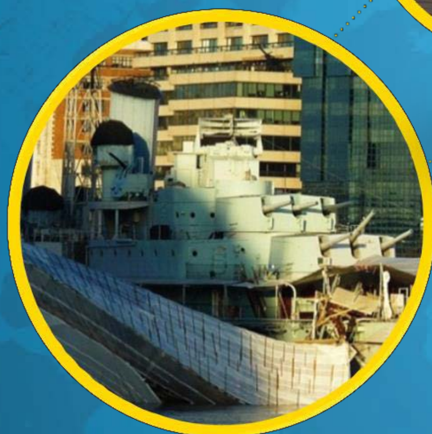
Enterprise Risk

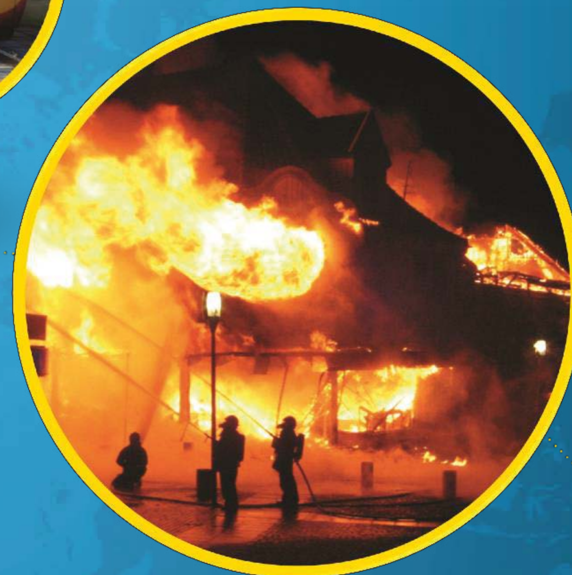
Spring 2017 / www.enterpriseriskmag.com

The official magazine of the Institute of Risk Management

Bigger picture: risk visualisation techniques / **Friending social media:** seeing risks and rewards / **Watch the back door:** focus on defence / **On the rise:** salaries increase / **Drone wars:** commerce or criminality

The talking cure: Wellcome Trust's Fiona Davidge explains her dialogic approach to risk management





Enterprise Risk

Spring 2017

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

Editorial

Cool for cats

As stock market flotations go, Snap is having a rollercoaster ride. It is the parent company of the social media company Snapchat – the video and image sharing platform. The app became popular because the messages self-destruct a few seconds after users send them, ensuring added privacy.

At the time of going to press, wags in the media are writing that a lot of the initial value on flotation seems to be disappearing just as quickly as one of the apps' messages. Yet much of the volatility is probably down to traders betting on the future direction of the company's share price – initially valued at $24bn by NASDAQ, the US exchange favoured by tech companies.

The business' disclosure to regulators revealed that on revenue of about $404m, it made a loss of $515m. So, that is some valuation.

Its rate of growth is slowing, but investors seem to buy into the "cool" factor around the teenage demographics of many of its users. Snapchat is said to be working on exciting new ideas to keep its audience interested, engaged and – crucially – looking at advertising.

> **One of the key things these apps provide is a free messaging system for different networks**

But is that how teenagers really use it? To take a totally unrepresentative sample, my two eldest teenage sons tend to take a blank image – the wall, for example – and send a message attached to that. Similarly, with Facebook, they never post anything to the site, but use the messaging function to contact friends who congregate around that platform.

One of the key things these apps provide, then, is a free messaging system for different networks of friends.

In that sense, social media can be a very powerful communications tool, as Alexander Larsen explains in this issue of *Enterprise Risk* (see pages 18-21). So much press coverage is devoted to the risks – reputation and otherwise – inherent in social media use, that risk managers are perhaps ignoring its obvious strengths as a risk management tool.

In the emergency response field, there have been some successes. During earthquakes in Japan, Facebook and Microsoft worked to help separated family and friends contact each other, and to communicate with relief organisations. Larsen suggests several ways that risk managers can begin to build a social media risk strategy.

It may never be worth $24bn, but risk managers taking this route could develop an invaluable tool for bringing people in their organisations together around the risk agenda. That would be cool.

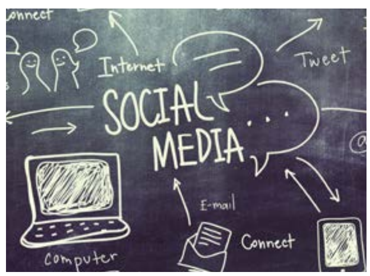
Arthur Piper
Editor

Contents

Spring 2017


10


14



18


22


26


30

FEATURES

REGULARS

Spotlighting director disqualification

The public interest in seeing directors punished for wrong-doing is growing, especially under new competition law regulations, says Nicola Crawford

We recently saw the first director disqualification under competition law. That underlines how bribery, corruption, competition law and slavery have become much more important elements of the risk landscape and shouldn't be ignored. Ethical and legal behaviour should be embedded in the culture of all organisations and not just for the fear of legal action.

There have been a few high-profile cases featured in the press recently where companies have clearly crossed the line and retailers seem to be increasingly in the spotlight. This latest case follows the first director disqualification because competition law was broken. A managing director of an online poster supplier gave an undertaking not to act as a director of any UK company for 5 years for their part in an online price-fixing cartel.

A director of a company that breaks competition law can be disqualified from acting as a director of a company, or carrying out other specified roles in relation to a company, for up to 15 years.

Of course, competition law is there to protect the consumer, stakeholders, markets and also the supply chain – healthy competition benefits us all. It creates free and transparent markets in which to do business in an environment where competition is fair and honest.

There is not only risk of litigation but also the long term damage on the brand and reputation of an organisation which could take years to repair. In the world of 24/7 social media your customers and competition will be doing a lot of talking on your behalf – increasing the reach of any news coverage or perceived wrong doings. In fact, you can read about how to better handle the risks of social media – and take advantage of its unique capacity to communicate in this issue of the magazine – see *Friending social media*, pages 19-22.

> **Ethical and legal behaviour should be embedded in the culture of all organisations and not just for the fear of legal action**

Our recent joint *Competition Law Risk Guide* (jointly produced by the IRM and the Competition and Markets Authority (CMA) features up-to-date case studies with key learnings and examples of best practice to help risk professionals navigate UK competition law it also offers some powerful recent and relevant case studies to highlight both unacceptable business practices and show just how easy it can be to get into difficulties if the risks are not properly understood and managed – compliance should be embedded from the top down.

Copies are available from the IRM website.

Trending

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

Show me the money

The average salaries for different categories of top risk management positions*

Top
Quantitative risk analysis
£180,000+

Bottom
Credit risk control
£130,000+

Morgan McInley, 2017 Risk Management Salary Survey Guide

*Based on being an MD with 10 years' service or more.

How good are chief risk officers at defining risk appetite?

Chief risk officers say they find the following areas "extremely" or "very" challenging when it comes to defining risk appetite

"Measuring strategic risk requires an institution to assess the overall risk posed by, and to, its business strategy"

Defining risk appetite for reputational risk
49%

Defining risk appetite for strategic risk
48%

Allocating the risk appetite among different business units
38%

Translating the risk appetite for individual risk types into quantitative risk limits
37%

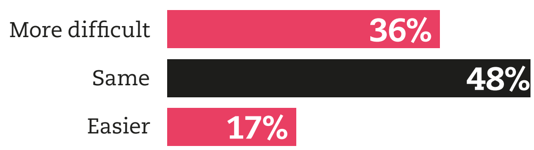
Defining risk appetite for operational risk
27%

Source: Global risk management survey, tenth edition. Deloitte University Press

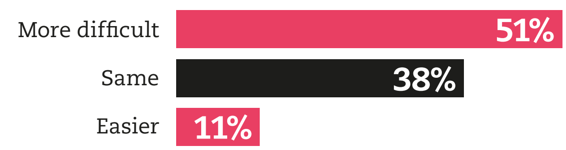
It's getting more difficult to forecast risk

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

Difficulty of forecasting risk today versus three years ago (2013)



Anticipated difficulty of forecasting risk three years from now (2019) versus today



> **Interconnected trends in geopolitics, technological advances, global economic integration, social instability and climate change, mean that the manifestation of one risk is increasingly likely to influence others with unforeseeable impacts**

Source: 2017 AFP Risk Survey

Large US companies most lucrative targets in cyberattacks

The US is the most popular destination for cyberattacks, and the most lucrative

Companies reporting one or more attacks in the last year

	Small companies Below 250 employees	Large companies Above 250 employees
UK	48%	59%
US	60%	72%

Average losses suffered

	Smallest companies Below 100 employees	Largest companies Above 1000 employees
UK	£25.7k	£62.7k
US	£23.9k	£83.0k

Source: Hiscox Cyber Readiness Report 2017, all dollar sums converted into pounds

The talking cure

Fiona Davidge is part of a two-woman risk team at the £20bn science funding charity Wellcome Trust. She explains how her dialogic approach to risk management is helping the executive team understand and deal with their strategic and project risks

BY ARTHUR PIPER

"The biggest thing we do as risk managers is talk," Fiona Davidge, Enterprise Risk Manager at the Wellcome Trust, says. "We own no risks within the risk team. Our job is to support others to make decisions."

With over £20bn of assets in its investment fund, Wellcome's decision whether to back a particular piece of research isn't trivial. As the world's second largest charitable funder of research into human and animal health, Wellcome awards nearly £1bn a year to an increasingly global and collaborative scientific community. Its funding not only helps shape the type and nature of global research into health, but influences the very direction of scientific research across a range of fields.

Over the past ten years, for example, about 20% of Wellcome's grants have gone into genomics – the study of the structure and function of DNA. It's no exaggeration to say that the genomics projects co-funded by the body – including the Wellcome Trust Sanger Institute and the Francis Crick Institute – have helped make the UK a global centre of excellence in the field, as well as enabling a range of international scientific collaborations. Inevitably, that influences what research takes place in the science community.

> **Your risk management has to be part of competent decision making. If that's not in place, that's your biggest risk**

> We are facilitators, enablers and here to support – not to throw up stops

"We are conscious that if we shift strategy, we have to engage with the community that we are funding and to explain our decisions to those who may be missing out," Davidge says. "We have to be clear and comfortable with what we are doing – it's a matter of reputation." Wellcome also has a remit to engage with the public – both through its collections, library and art-science collaborations, and through engagement with public health research policy.

In fact, Wellcome's strategic objectives are undergoing a period of change. While it is based in London, and with no current plans to move, the research projects it funds have become increasingly geographically global, but with particular focus on Africa, India and South East Asia. That is because healthcare solutions to epidemics, antibiotic microbial resistance, and other problems are not unique to countries or continents. Wellcome funds initiatives in other countries, often through UK academia, to bring together the best talent in the world in the most relevant places. "If we want to make an impact on the HIV epidemic, we have to build research capacity in those countries where the disease is prevalent , and accept and manage the greater risks associated with funding into those countries," Davidge says.

Proactive

And Wellcome has become more proactive, acting as a catalyst for projects that it could not fund by itself. That has seen it working with the world's largest philanthropic health funder, the Bill and Melinda Gates Foundation, and governments from around the world. The Coalition for Epidemic Preparedness Innovations, a global partnership to prevent epidemics with new vaccines

– launched at Davos this January – is the latest of such schemes.

This has shifted some of the skill sets Wellcome needs in-house. It has a sophisticated and well-run funding strategy. As one would expect, its assets are diversified and there is a dedicated team running the portfolio with Sarah Fromson, Davidge's boss, responsible for investment risk. But delivering these newer, collaborative projects requires it to develop its programme management skills. That can be tricky, says Davidge, because the project might not be a tangible thing such as a building, but a concept – how to best model disease, for example. "Yet it is still a programme of activity and we need people who can make that happen and help free up scientists to develop the science," she says.

"Your risk management has to be woven into that – it is part of competent decision making," she says. "If that's not in place, that's your biggest risk."

A big part of Davidge's role is to maintain strong links with the senior project members. It can be a challenge to keep on top of what is happening because a greater emphasis on collaboration – driven, it should be said, by how science works today, rather than by any ideology coming from Wellcome – has meant that project teams are comprised of people both within the charity and within its external partners. In the past, Davidge may have been able to speak to the head of science at Wellcome to find out what was happening within that division, she explains. Now, things are more complex. The organisation's head of science may be working on several projects simultaneously, each comprising networks of global scientists. Davidge needs to ensure all the senior people in these projects have thought about the risks of what they are doing and have plans in place to deal with any issues that may arise.

Facilitators

"It's my job to ask how project leaders have thought about risk management and to advise them that it's best to build risk management in from the start," she explains. "We are facilitators, enablers and here to support – not to throw up stops. It's about getting people to go into projects with their blinkers off and actively look at what issues are associated with their initiatives so they can hopefully mitigate them before they become a problem."

Where project leaders are involved in several initiatives, Davidge encourages them to think how risks that could arise in one could impact work in another. That could mean looking at how internal or external staff resources are deployed and how they interact when the inevitable problems arise from time to time.

At a strategic level, Wellcome has a risk register, which is updated every quarter for due diligence purposes. It provides a useful snapshot for where the organisation is at a particular point in time, but, says Davidge, "it's not an end in itself." The organisation does not have a risk committee. The two-person risk team reports to the Chief Financial Officer Tim Livett. And there is no risk management software. While Davidge can see the obvious benefits for managing huge capital projects with software, or compliance-related exercises in financial services organisations, she believes it can just as easily get in the way.

Unlike many other charities, Wellcome does not have a large infrastructure in terms of high-street retail outlets staffed by employees and volunteers, nor does it need to fundraise with all the hassle that can bring. Wellcome was founded from the bequest of a single donor, Sir Henry Wellcome, in 1936. Its main asset was Sir Henry's company, Wellcome Foundation, and it pursued its aims from the profits of that business. After floating on the London Stock Exchange, the Wellcome sold its final major shareholding in the business in 1995 to Glaxo – now GlaxoSmithKline – by which time it had assets worth £3.4bn.

Governance

The charity's board of governors comprises a mix of top-flight scientists and business and investment executives. Unusually, it pays its trustees because of the high level of responsibility they carry both in terms of signing off on major initiatives and in helping to approve Wellcome's long-term strategy. They are supported by the

IRM CHARITY GROUP

The IRM Risk Special Interest Group was established over 10 years ago to provide practical guidance for charities about managing risk and opportunities, and for sharing knowledge, tips and best practice amongst sector professionals. Its overall aim is to increase the sector's knowledge of risk management best practice, explore practical solutions for managing sector challenges (such as new regulatory requirements), and provide a forum where risk professionals can meet to learn from one another and share up-to-date risk management practice.

To get involved visit: https://www.theirm.org/events/special-interest-groups/charities

> To be able to get on with people and articulate yourself verbally and in written form, to influence and challenge, are absolutely key

executive team, which puts forward the strategy and executes it.

The risk team meets individually with every member of the 15-strong executive team on a quarterly basis. Each executive brings their risk champion and they talk about what is happening, what significant changes are coming and how those things might affect their activities. Between them they create a risk report that goes to the CFO. Quarterly, the executive leadership team meets to consider all of these reports together, which provides a more collective view of the risk environment.

"The value of the process is that we provide half an hour in someone's busy, valuable time where they can explicitly focus on risk," she says. "They can think what their risks are, how those risks are being managed – and we can provide challenge as to whether they have really covered everything and whether the measures they have taken are effective. Would we have that thoughtfulness if I was sitting there filling in a little bit of software? My experience is 'no'."

Eighteen months ago, an internal audit provided by an external consultancy found that the whole of the executive team was engaged with and knew what risks it faced. For Davidge, that is confirmation that her pared-down, dialogic approach works. "In the risk profession, we can put far too much onus on our processes when it comes to talking about strategy, direction and purpose."

Davidge started her career as a business resilience and security manager at Thames Water in 1998. There was no corporate risk programme and when the business decided to implement one, she was handed the task by her then boss who was close to retirement. Thames Water supported her through the IRM's Diploma. When she moved to Transport for London (TFL) in 2007, it was as senior corporate risk manager. She had been working on the British Standards Institute Committee for its business continuity standard (25999), and she was invited to work on the risk committee standard following her move to TFL. Last year, she won an award for her work on ISO 31000 from the International Organisation for Standardisation, which she has sat on for about seven years.

"From a risk perspective, working on ISO standards means you get viewpoints on risk from around the world – not just at meetings, but over coffee and in the hotel where you meet," she says. From a practical point of view, she says the experience has helped her hone her negotiating and consensus skills because of the wide range of personalities and viewpoints in play.

She is a member of the IRM's Charity Special Interest Group (See Box out) and has given input into the guidance the group produces. While she believes technical knowledge is important, her advice to professionals just starting out on their careers is to focus on the practical. Thoroughly understand the business's objectives and how the organisation runs, she says. And develop your communication skills. "To be able to get on with people and articulate yourself verbally and in written form, to influence and challenge, are absolutely key," she says. "Risk management is a dialogue."

Seeing the bigger picture

Risk registers often fail to convey the systemic complexity in enterprise risks. Visualisation can help reveal the bigger picture

BY NICO LATEGAN

Writing as a risk professional with 15 years' experience, I have a confession to make. I loathe risk registers. Let's face it, they are boring, one dimensional, and poorly-prioritised lists that lack context and often serve to satisfy a requirement rather than a purpose. Risk registers can be useful in some contexts, but I believe a risk visualisation approach is a far better way to accomplish the aims of risk management and support better decision making. So, what is risk visualisation, and how do we implement it?

Risk visualisation is a relatively new concept, which traces its roots back to data visualisation. Data visualisation is itself a broad theme, ranging from charts and graphs to geographical mapping and highly-stylised infographics. It is supported by a mature set of applications, from the ubiquitous Microsoft Excel, to sophisticated business intelligence and big data analysis tools.

The late Dr Hans Rosling pioneered the concept of telling compelling stories by combining data visualisation and the fourth dimension – time. His TED talks, "The best stats you've ever seen," and the shorter, "Hans Rosling's 200 countries, 200 years, 4 minutes," are both classic examples of his approach, which you can view on YouTube.

> **Tools now exist to enable the creation of richer, more context-aware risk visualisations based on information captured through normal risk identification and analysis processes**

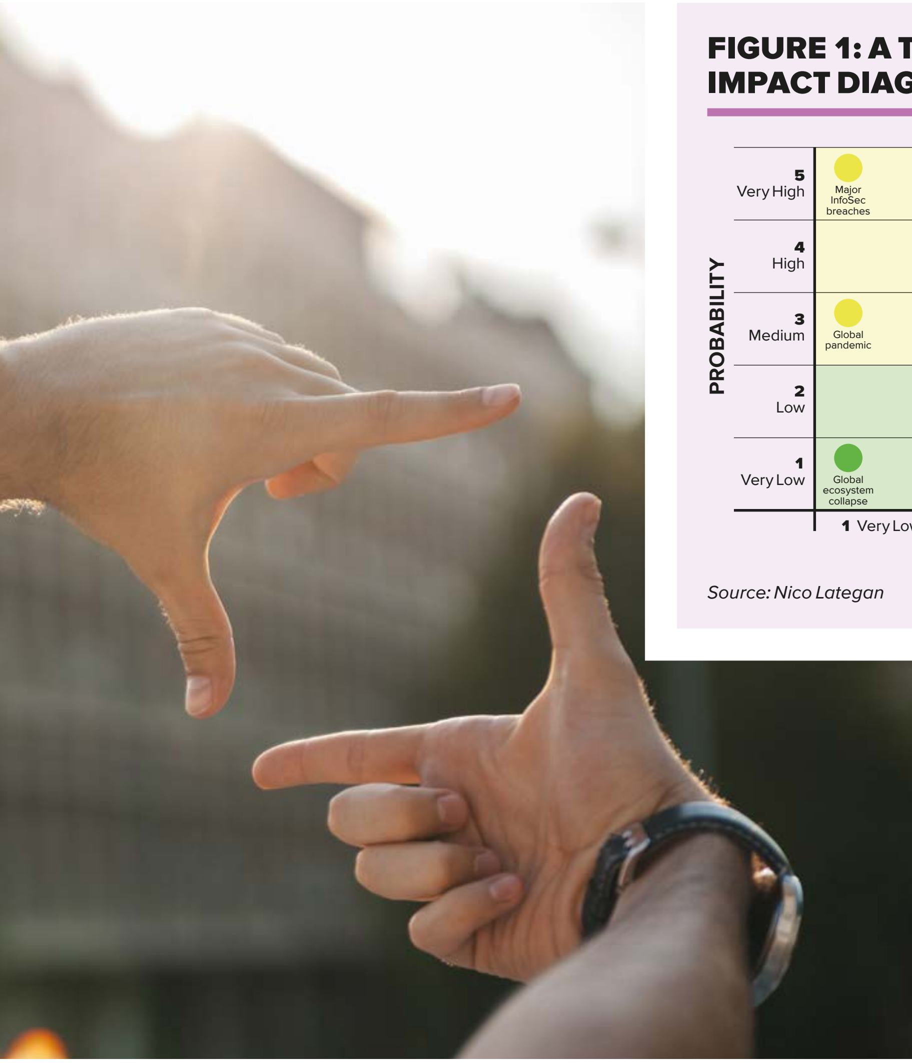
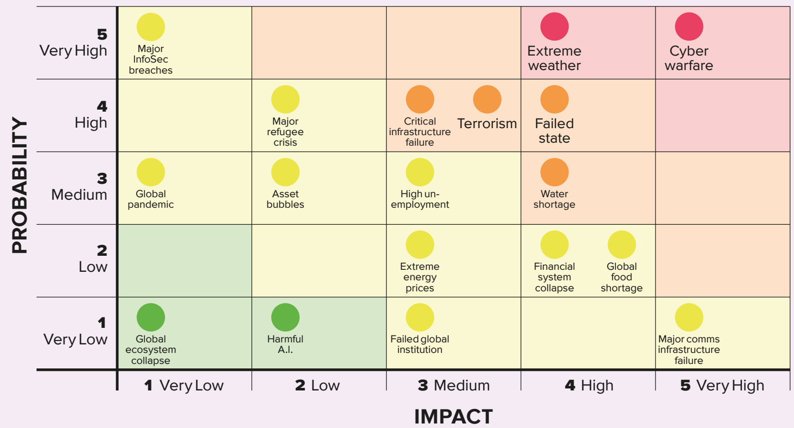


FIGURE 1: A TYPICAL PROBABILITY IMPACT DIAGRAM (PID)



Source: Nico Lategan

Risk maps

An early version of risk visualisation has been with us for decades in the form of the risk heat map. It is usually depicted in a three-by-three, or a five-by-five matrix. Probability, or frequency, runs along one axis, while impact, or consequence, runs along the other. The map is often referred to as a probability impact diagram, or PID.

A heat map is a slight improvement on the traditional risk register approach in the sense that it transfers a lot more information to the reader at a glance. Users of the information can intuitively zoom in on the risks requiring intervention through the use of colour, size and position of the risk elements on the grid. Beyond this however, heat maps are somewhat limited in providing context, conveying systemic complexity and aligning risks to organisational goals.

Another form of risk visualisation includes shading areas on a geographical map to indicate risk levels, or using dots of varying sizes and colours to indicate location-specific hazards.

These are more useful for organisations or institutes where a geographical context is important, such as those showing the risk of travelling in different countries. They simplify a large amount of data into an impactful image that draws attention to key areas of risk.

Current developments

Tools now exist to enable the creation of richer, more context-aware risk visualisations based on information captured through normal risk identification and analysis processes. These can model the systemic nature of risk causality and interconnectivity. To understand this concept, let's examine the global risks we face in 2017.

Global risks do not exist in isolation. Those that materialise could have an exacerbating effect on the materialisation of others. For example, any combination of risk categorised as asset bubbles, extreme energy prices, water shortages, or financial system collapses could result in the risk of a failed state. This in turn can exacerbate the risks from terrorism, a major refugee crisis, further water shortages and extreme energy price increases.

This concept of systemic and interrelated risks can equally be applied to enterprise risks in an organisation. For example, cyber threats can be affected by, and in turn affect, the materialisation of related risks across the organisation. In this way, risk visualisation highlights the need to reach across organisational silos to effectively manage and mitigate the strategic threats facing an organisation.

Furthermore, risk visualisation can illustrate a rich array of information across multiple dimensions, including – but not limited to – risk proximity (how quickly risks are likely to materialise), categorisation (against predefined risk categories or organisational objectives), control effectiveness (the effectiveness of mitigations currently in place), impact quantification (the actual numerical value of impacts measured, for example, in pounds sterling) and risk trajectory (risk exposure reduction over time). In these circumstances, risk visualisation can be a powerful aid in getting a message across to decision makers, enabling them to prioritise and highlight appropriate risks for immediate attention or identify opportunities for collaboration on risk mitigation efforts.

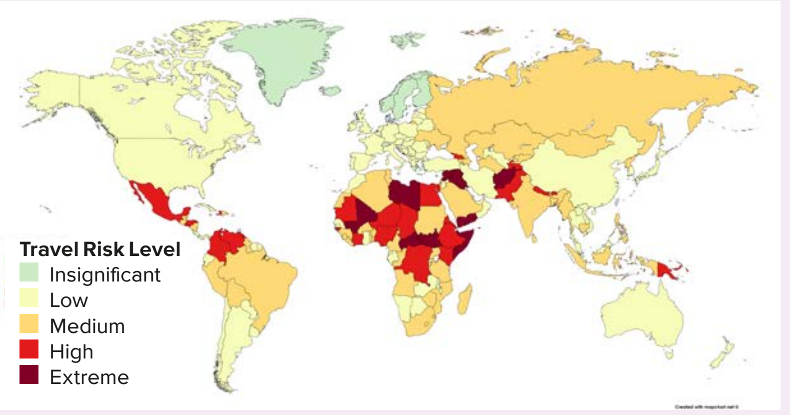
Benefits

Risk visualisation is far more engaging to users of risk information than simply relying on risk registers to convey the same message. This is due in part to the rich context of the risk information combined with the ability to tailor the information to suit different audiences. Interactive visualisations can be used to highlight risks that exceed an organisation's risk appetite, risks with poor controls, risks against certain key objectives, or any combination of such criteria.

Visualisations can also be used to present high-level strategic risk information to executives, whilst retaining the ability to drill down into the details for appropriate audiences. Increased engagement and understanding of enterprise risks leads to better decision making at all levels of the organisation, from frontline staff all the way up to the board room.

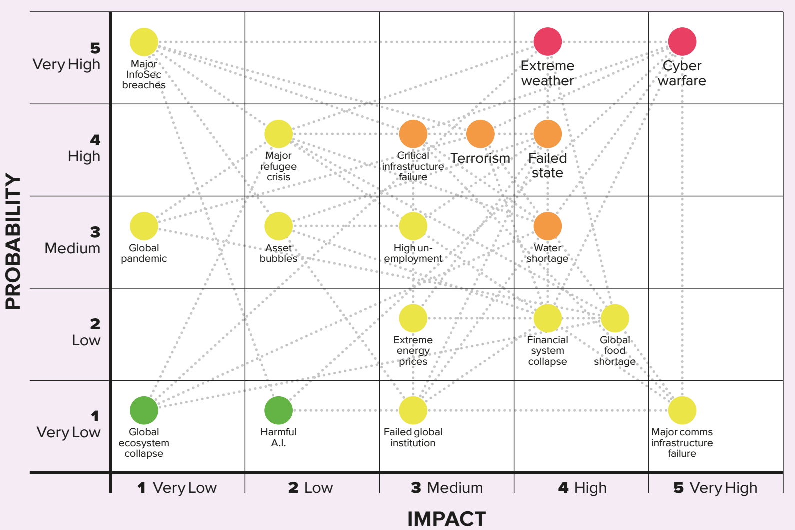
Systemic modelling of risk interconnectedness has a profound effect on the way people perceive risk. Instead of focussing solely on risks in their own silos, there is a genuine understanding of the strategic nature of enterprise risks, and this encourages a collaborative approach to risk mitigation.

FIGURE 2: TRAVEL RISK MAP



Source: Nico Lategan

FIGURE 3: SYSTEMIC VIEW OF INTERCONNECTED RISKS



Source: Nico Lategan

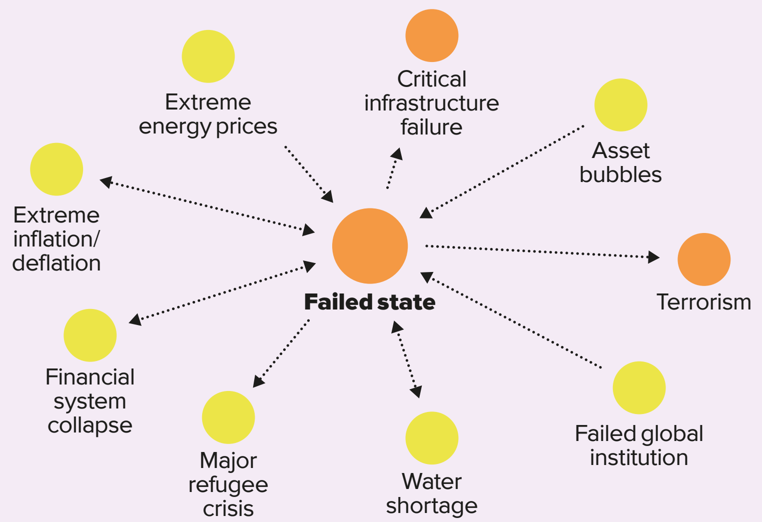
Implementing risk visualisation

Technology is often the easiest component of adopting a risk visualisation approach. It is far harder, but absolutely crucial, to implement a comprehensive risk framework that encompasses all the elements of an ISO 31000 approach. The framework should include a methodology for comparable analysis of risks against stated objectives and a defined organisational risk tolerance and/or appetite.

The old adage applies here – garbage in, garbage out. Risk visualisation will only ever be as good as the information behind it. Designing, communicating and embedding this framework successfully allows the right information to be collated in order to build a risk visualisation model that can support effective decision making, and ultimately, effective risk management.

Once a risk framework is in place, it is relatively straightforward to design a risk visualisation strategy based on information captured through the risk process, organisational structure, and desired outcomes from adopting a risk visualisation approach. It is important to note however that there are some technical design issues to consider. Examples include the specification of information required, the flow of data from the point of capture through to storage and presentation, the integration between various databases and toolsets, and whether these are managed on-premises for better security or

FIGURE 4: THE SYSTEMIC NATURE OF INTERCONNECTED RISKS



Source: Nico Lategan

GETTING STARTED

Steps for implementing a successful risk visualisation approach:

1. Design and implement a robust risk framework based on ISO 31000
2. Conceptualise the desired risk visualisation outputs
3. Socialise a proof-of-concept with key decision makers and users of risk information
4. Communicate the benefits, actions needed and implementation date of risk visualisation
5. Build and roll out final risk visualisation solution, with training and support in place.

> Systemic modelling of risk inter-connectedness has a profound effect on the way people perceive risk

in the cloud for easier access and collaboration between entities.

Risk visualisation technology can be inexpensive relative to commercial, off-the-shelf enterprise risk management solutions, and fairly easy to implement. It is flexible enough to be configured to reflect organisational and risk process changes, and can model threats, opportunities, causes, consequences, controls, improvement actions, key risk indicators and anything else organisational risk processes require.

Challenges

People can naturally be sceptical about the benefits of new approaches and technologies, and risk visualisation is no exception. With risk visualisation, however, seeing is believing. It is easier to convince decision makers of the benefits of adopting a risk visualisation approach using a well-designed proof of concept rather than presenting a standard business case.

Providers of risk information can be another source of inertia preventing the risk process from evolving. This is especially true once they come to the understanding that risk visualisation will expose data quality or risk maturity shortcomings to senior management. Working with them to set a realistic deadline for the collation of risk information with the expectation that the board will be shown all risk visualisations can be a catalyst for positive change in this area.

The future

Risk visualisation is the natural evolution of and ultimately a replacement for traditional risk registers. It is a far more engaging and useful approach when attempting to understand the context of systemic risks, prioritise risks, and tailor risk information to audience requirements. Risk visualisation has the added benefit of encouraging providers of risk information to comply with risk processes to ensure current and detailed risk information is presented to the board.

The next step requires organisations to embrace the concept of visualisation to the point where risk visualisation is no longer an isolated approach, but is linked to every part of a business including strategy, assurance, compliance, business performance and change programmes. This pervasive embedding of risk management across an organisation to achieve business success is the ultimate aim of risk management. Enterprise risk professionals with their strategic overview of their respective organisations are uniquely placed to influence the development of approaches that can enhance business success. Risk visualisation is the first step in this direction.

Nico Lategan is an award-winning risk visualisation expert, chairman of the IRM's Milton Keynes Heads of Risk Forum, a senior enterprise risk specialist at Network Rail and contributor to HMG's Risk Improvement Group. The opinions expressed in this article are the author's own and do not reflect the views of Network Rail or Her Majesty's Government.

Friending social media

How can businesses get the most from social media, at the same time as avoiding its potential risks?

BY ALEXANDER LARSEN

There is no doubt that involvement in social media activities is the source of a great number of risks to companies. But there are also risks to not having an online presence. Companies who are not active on social media could surrender ground to competitors, fail to attract a younger customer base, and could end up either not building a reputation – or slowly losing an already strong one.

Organisations cannot avoid social media risk by pursuing a policy of non-participation. Customers, journalists, or the public in general, can easily and quickly point out major faults with a company product or service to a large number of people. With enough attention, that can severely impact brand and reputation. Additionally, tweets can be sent out instantaneously from shareholder meetings, board meetings, or from interviews, leaving little time to prepare for a response. It is vital that organisations manage social media risk proactively.

Companies generally have two main concerns about social media. The first relates to risks to the organisation. For example, an employee that uses social media badly can expose a company to intellectual property and data leakage by saying too much about products and services. Or, extreme views expressed by staff on a company's social

> Organisations cannot avoid social media risk by pursuing a policy of non-participation

> A social media policy can be short and sweet, or quite long and detailed

Below: Managing the wide range of existing social media platforms should be straight forward with effective ERM.

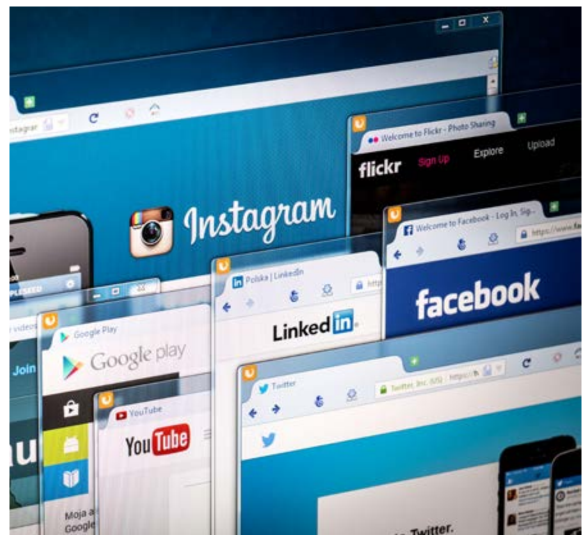


Image credit: REDPIXEL.PL / Shutterstock.com

media platforms could be interpreted as a reflection of the company's own values. Viruses, hacker threat, or phishing attacks can all be introduced into the company network because an employee's work and private login passwords are identical.

The second relates to the organisation's social media presence. Where companies are active on social media, for example by having a forum, message board or Facebook page, they are exposed to any customers, members of the public, or disgruntled staff posting negatively about the company, or hijacking company-led social media campaigns. Internally, risks can arise from the inefficient use of social media. Often companies will have a presence on social networks but rarely update them, or have inconsistent or conflicting information, such as contact details, across the various networks. This can frustrate users and lead to missed opportunities.

Understanding social media

Keeping on top of social media-related risks should be straight forward if there is an effective enterprise risk management (ERM) programme in place. With reputation risks being at the top of corporate risk registers and board agendas, there is a need for the constant monitoring of reputation risks (such as social media presence) and mitigation actions should be implemented where needed.

But, as with all risks, you can manage them best when you identify them as early as possible – preferably before you even begin to have a social media presence. The best form of prevention is to be well prepared. When entering into social media, a company needs to focus on the purpose of doing so in the first place. Is it to attract talent, or improve customer engagement, for example? Once this is established, objectives can be set for the initiative. Different objectives will require varying approaches, not only to achieve the desired success, but also in how to mitigate the risks.

One of the mistakes many companies make when developing a social media plan is that it is often left to a single department, such as IT or marketing, rather than to a multi-disciplinary team. Best practice indicates that representatives from risk, legal, compliance, management and any other affected departments should all be involved with the process. Having such a team in place will allow for proper preparation in terms of understanding the risks of using social media, and how to mitigate them, without having a negative impact on the initial objectives of the plan. Once a robust plan is ready, senior management should be informed, educated and commitment must be obtained.

Mitigating risks

Some companies have a total ban on employee access to social media. Others may decide that only certain sites are appropriate, and could help with the company's online presence. If a business bans specific social media sites, it should consider the consequences of creating an unhappy workforce. An alternative is to have a completely open social network policy, but with an opt-in programme, whereby staff agree to "friending" the organisation on their social media sites in return for being able to access it from work.

If employee access is given, there are some common steps companies can take to mitigate social media risk. First, the company should develop a social-media policy and train staff in its use. A social media policy can be short and sweet, or quite long and detailed. A company should consider having one for employee use of social media as well as a corporate social media policy (for those working with social media on behalf of the company). These should include an outline of the do's and don'ts when posting online, information on the safe use of social media, off-limit subjects or data, as well as the consequences of being in breach of the policy. The legal department should be of use here.

Second, a company should monitor the comments and behaviour of staff on an ongoing basis in order to avoid reputational damage, or even from being held liable for comments made by employees. When using social media sites, there is a risk that staff will upload sensitive data, perhaps by accident, or that they download files which can contain viruses. IT will often restrict downloading or uploading on company computers, as well as securing sensitive files. Enforcing virus and malware protection is another way that IT tends to protect a company but this needs to be confirmed by the team. This is another reason why having a multidiscipline team that includes IT is so effective.

Finally, dealing with customer complaints in an appropriate manner is vital. Companies should avoid directly deleting comments or negative posts, as well as avoiding aggressive or negative responses. Instead, a company should try to bring the conversation to another platform and try to deal with the complaint directly. Training will be a key element to successful complaints handling on social media.

Image credit: Hadrian / Shutterstock.com

> **"Used in the right way, social media can allow risk managers to tap into an organisation's most valuable resource – its people**

Force for good

Something that risk managers may overlook with regards to social media is the potential benefits it can bring to risk management. Used in the right way, social media can be a strong tool for managing risks and opportunities, allowing risk managers to tap into an organisation's most valuable resource – its employees.

Google is a prime example of using social media tools to minimise risk and maximise opportunity. For example, Google Moderator allows project leaders, R&D teams and top management to post their ideas, initiatives or innovations for

Above: Social media can be a powerful communication tool, so companies need to make sure they understand how to control it properly.

anyone within the organisation to challenge or ask questions about. Voting within the tool allows many of the questions most relevant, or most concerning, to employees to be pushed to the top of the pile.

Not only does the use of such a tool involve the workforce, and thus increase staff morale, but it can drive the success of major change management initiatives (for example after a merger) if everyone feels that their voice is being heard and considered. It can also potentially highlight key risks to a product launch that may not have previously been identified by a project team working on its own. It was so highly thought of that the Obama administration used it when transitioning into office to make the process of change more successful.

A couple of other initiatives that Google has implemented include Google's weekly all-hands meetings, where employees ask, through social media tools, questions directly to the company's top leaders and other execs about any number of company issues. Again, this concept can be used by risk managers to capture risks and opportunities from across the organisation. Perhaps a more obvious risk tool for risk managers would be to implement something similar to the Google Universal Ticketing Systems – GUTS – which allows users to report issues, and is then reviewed for patterns or problems. Adapting this to a more risk-based solution could really support an organisation in identifying risks or trends before they happen. It can allow the reporting of risks from anyone in an organisation, bypassing more senior employees who may try to stop these risks from being reported. Such a tool could serve as a tool to escalate risk past local management.

Continuity

Business continuity can benefit greatly from social media by, for example, connecting stakeholders to internal staff during an incident. Many countries are already using social media, such as Twitter or Facebook, to issue hurricane and tsunami warnings to citizens on top of the more traditional alarms. This not only informs the local population who are in immediate danger, but also allows family members or friends who are signed up to the service to receive these notifications.

A similar approach should be considered by companies when it comes to spouse management during a major incident. Companies who operate in dangerous locations such as war zones, politically unstable regions, or on offshore oil platforms, should consider offering employees' spouses the opportunity to connect to a specific company emergency social media page. This page can be the main hub of communication for spouses should an emergency occur. Not only will they get regular and factual updates, but they can post questions and even comfort each other by having a community of people in similar situations as themselves. This could be extended to include sites for connecting with stakeholders during an incident whether it be suppliers, clients or even the media.

Social media has already been used successfully during earthquakes in Japan. Pages were set up on Facebook to keep the public up to date, whilst Microsoft worked with partners to create local applications such as J!ResQ – a smart phone application for emergency contacts – to help people find family and friends and to aid relief efforts with aid agencies. Looking more internally, business continuity plans will have steps that include informing staff of job status, whether to stay at home, work from home, work from an agreed second location, or even return to work. Using an internal social media tool can greatly improve the efficiency of this message compared to more traditional methods such as a phone call to every staff member.

Getting over initial worries about the use of social media can turn many of the risks associated with these technologies into opportunities. By carefully working through the threats and mitigating risk, risk managers can help their businesses benefit from these powerful tools.

Alexander Larsen, president of Baldwin Global Risk Services www.Baldwinglobal.com. Contact: al@baldwinglobal.com

Is anyone watching the back door?

Companies need to strike the right balance between bringing in the cash, and preserving value in the business. Is a new focus on corporate defence in order?

BY SEAN LYONS

Success in business in the twenty-first century is increasingly associated with the delivery of stakeholder value in the short, medium and long term. Few would argue that, in theory at least, corporate strategy should therefore address the subtle balance between short-term value creation (offence) and long-term value preservation (defence) in order to deliver sustainable value. In this context value creation is regarded as the focus on bringing the dollar in through the front door, while value preservation is regarded as the focus on preventing the dollar from leaving through the back door.

Twenty-first century stakeholders typically expect that their organisation will consistently deliver sustainable stakeholder value. But in the face of continuous corporate scandals involving such household names such as Volkswagen, FIFA, and Wells Fargo, many stakeholder groups are now showing signs of serious concern. Stakeholders are beginning to question the adequacy of the measures currently being undertaken by their organisations in order to safeguard their interests and to protect their value.

> **Corporate defence is synonymous with value preservation**

> The challenge now facing risk professionals is to have the courage to stretch outside their risk-centric comfort zones towards a more holistic view of the organisation's corporate defence requirements

Value preservation imperative

In light of this scrutiny, in far too many organisations an imbalance exists, what is referred to as a value preservation deficit. This deficit can begin with the disconnect between value creation and value preservation efforts at a strategic level in many organisations, and, as a result, this disconnect tends to cascade down to tactical, and operational levels. Unfortunately, in such circumstances the issue of value preservation is more likely to be implied or addressed as an afterthought, rather than being considered as an essential element of an organisation's corporate strategy. In this regard, many organisations fail to understand or appreciate what is referred to as the value preservation imperative. Put simply, an organisation's obligation to its stakeholders to take adequate steps to help preserve value and help defend against value erosion, reduction, or destruction.

Corporate defence is synonymous with value preservation. The umbrella term corporate defence programme represents an organisation's collective programme for self-defence, and it reflects how it is organised to safeguard and protect stakeholder interests. Effective corporate defence, however, is not easy as it requires the alchemy of both science and art in order to effectively defend the organisation and its stakeholders against potential hazards which could have a detrimental impact on stakeholder value. In practice, every organisation will have some form of corporate defence programme in place whether by accident or design. This can range from a formal structured programme, to an informal unstructured programme, depending on the organisation in question.

Corporate defence theatre

Although the concept of corporate defence appears to be intuitively understood, its precise requirements do not appear to be fully appreciated in many organisations resulting in corporate defence theatre, which is merely the illusion of corporate defence. Everyday in the media, stakeholders are informed of corporate scandals whereby previously respected organisations have found themselves in difficulties of their own making. These scandals are often the result of events which in retrospect the organisation could have and should have better anticipated, prevented, detected or reacted to.

Not surprisingly, post-mortem investigations into the causes of these scandals consistently expose deficiencies and weaknesses in their corporate defence programmes which have led to unnecessary large scale losses, significant reputation damage, and negatively impacted on stakeholder value. These deficiencies and weaknesses can begin with the non-existence of a formal corporate defence programme. However, individual corporate defence issues can also have an impact. Typically examples of these issues can include failures in corporate governance, poor risk management, compliance failures, unreliable intelligence, inadequate security, insufficient resilience, ineffective controls, and failures by assurance providers. The existence of more than one of these issues in any given organisation tends to exacerbate the initial problem and can eventually result in exponential collateral damage to stakeholder value.

Logically if deficiencies and weaknesses in corporate defence programmes tend to result in corporate losses and failures, then improved corporate defence programmes can help better safeguard against the occurrence of such scenarios. What is needed is more robust and more effective corporate defence. Effective corporate defence requires the design and implementation of a comprehensive corporate defence programme which provides a multidisciplinary roadmap so that all corporate defence related activities are strategically aligned, tactically integrated and operating in unison towards the achievement of common objectives.

Comprehensive defence

A comprehensive corporate defence programme needs to address corporate defence requirements throughout the organisation, at strategic, tactical, and operational levels. It needs to be able to provide the complete picture of how corporate defence activities operate across the organisation's various lines of defence, all the way from the boardroom to the front-lines, and vice versa. It should help provide a holistic view of corporate defence and incorporate the management of eight critical corporate defence components (See *Critical defence components*). An effective programme involves aligning, integrating, and coordinating these interrelated disciplines and involves the collective management of these components throughout the enterprise in order to help maximise their potential value.

Each of these critical components address corporate defence from different and unique perspectives, and these form part of the necessary system of checks and balances required to help ensure that the organisation is taking appropriate measures to help preserve stakeholder value. Management of these components requires an

CRITICAL CORPORATE DEFENCE COMPONENTS

- **Governance:** How the organisation is directed, managed, and controlled all the way from the boardroom to the front-lines.
- **Risk:** How the organisation identifies, measures, and manages the risks it is exposed to.
- **Compliance:** How the organisation ensures that its activities are in conformance with all relevant mandatory and voluntary requirements.
- **Intelligence:** How the organisation ensures that it gets the right information, for the right purpose, in the right format, to the right person, in the right place, at the right time.
- **Security:** How the organisation ensures that it protects its critical assets from threats and danger, its people, information, technology, and facilities.
- **Resilience:** How the organisation ensures that it has the capacity to withstand, rebound, or recover from the direct and indirect consequences of a shock, disturbance, or disruption.
- **Controls:** How the organisation ensures that it has taken appropriate actions in order to address risk and to help ensure that the organisation's objectives will be achieved.
- **Assurance:** The system in place to provide a degree of confidence or level of comfort to the stakeholders that everything is operating in a satisfactory manner.

> Risk management practitioners have an opportunity to help their organisations evolve to a higher level of maturity in their corporate defence efforts

appreciation of the continuous interaction, interconnections, and critical interdependencies which exist between these specialist disciplines and the potential cascade of consequences which can result. It requires an understanding that these complimentary components continuously impact on one another in this increasingly complex corporate ecosystem. In fact the symbiotic nature of their relationships means that each contributes to, and receives from, each of the other components. Their collective management is required as recent developments in each of these disciplines has meant that the boundaries between these activities have become somewhat blurred, therefore it is now increasingly difficult to determine where one component ends and another begins. A comprehensive corporate defence programme can help provide the organisation with both defence-in-depth and defence-in-breath, thereby helping to create a more robust and resilient organisation.

The challenge

Enterprise risk management (ERM) is an essential element of any organisation's corporate defence programme and typically risk management practitioners are seen to be the driving force behind how their organisation routinely identifies, measures, and manages the risks it is exposed to. Very often, however, risk professionals tend to view the organisation's activities through a risk-centric lens (i.e. viewing issues in the context of risk elements). However, it is important to appreciate that viewing any issue through a risk-centric lens will provide a very different perspective than when viewing it through a compliance-centric lens or a resilience-centric lens. The challenge now facing risk professionals is to have the courage to stretch outside their risk-centric comfort zones towards a more holistic view of the organisation's corporate defence requirements.

This will involve ensuring that their organisation not only evaluates issues through a risk-centric lens but that it also views these issues through the lens of the other critical components, such as governance-centric, compliance-centric, intelligence-centric, security-centric, resilience-centric, controls-centric, and assurance-centric.

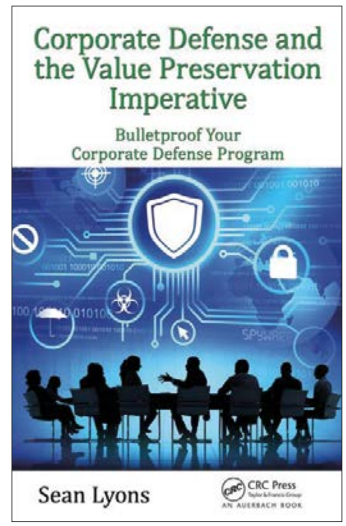
A risk-centric view impacts on all the critical defence components and vice versa. For example, governance risk refers to the risk elements associated with governance activities, while risk governance refers to the governance elements associated with risk activities, and so on and so forth. A clear understanding of the inter-disciplinary dynamics at play between each of these critical components is essential. Risk management practitioners have an opportunity to play an important role throughout this important learning process to help the organisation evolve to a higher level of maturity in its corporate defence efforts.

Incentives to improve

In the current economic environment, there is an increasing onus on each organisation to be able to successfully demonstrate that they are taking all reasonable steps to prevent unnecessary losses, to safeguard stakeholder interests, and to adequately protect stakeholder value. In November 2016, Professor Arnold Schilder, chairman of the International Auditing and Assurance Standards Board (IAASB) delivered a keynote speech at a conference in Brussels entitled, *The future of audit*. In this speech, he stated that "Understanding the business of the auditee, its corporate defence, and value preservation is a cornerstone of a robust audit".

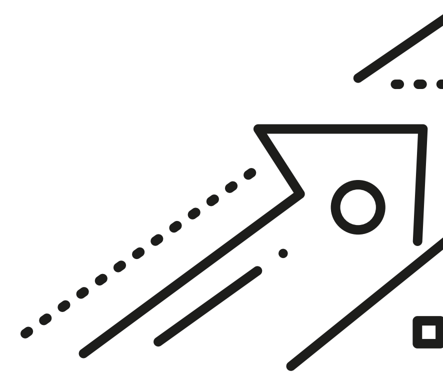
For certain organisations, the prospect of external auditors, rating agencies, and various regulators adopting such a focus when assessing their organisation will provide an adequate incentive to revisit their existing approach to corporate defence. For some organisations the prospect of better protecting stakeholder value by implementing a more robust corporate defence programme will provide them with sufficient incentive. While for others the prospect of actually optimising stakeholder value through improved performance and increased productivity will prove to be the primary motivating factor. Ultimately, an effective corporate defence programme can help to ensure that the organisation is fulfilling its fiduciary duties, legal obligations, and moral responsibilities, while at the same time helping to create durable value and sustainable economic performance.

Sean Lyons is the author of *Corporate defence and the value preservation imperative* published by CRC Press, 2016. For a 20% discount visit www.enterpriseriskmag.com



> **Enterprise risk management is an essential element of any organisation's corporate defence programme**

On the rise



Demand for risk managers with the right qualifications and skills is rising, along with salaries

BY NEIL HODGE

Demand for risk managers at both junior and senior levels is high at the moment, say recruitment experts, but those that can display sound business acumen and a keen industry awareness will stand out ahead of other candidates.

Recruiters say that the jobs market for risk managers is currently good – and getting better, particularly in sectors that traditionally employ risk and compliance professionals in large numbers, such as financial services. However, other industries are also on the look-out for good candidates, either for short-term cover on projects, or for full-time posts. Furthermore, companies are set to pay more for the right people: recruiters say that there has been a 5%-10% increase in most risk professionals' salaries over the past year.

Chad Lawson, associate director who runs the risk, compliance, financial crime and finance teams at specialist recruitment agency Robert Walters, says that the market to recruit risk professionals has picked up going into 2017, with a significant increase in new vacancies across the financial services risk market. He says that the bulk of these hires are "at the assistant vice-president/VP level, looking for experienced hires who have the ability to engage with senior stakeholders, but still not too experienced to be removed from the day-to-day risk management work."

Brexit has not had a noticeable effect on recruitment patterns. "The only effect we saw last year was a slowdown in recruitment volumes and permanent roles

> **It is a good time to be looking for a new opportunity if you are a risk management professional**

moving to interim roles due to uncertainty. We have not seen any sort of bias towards hiring UK risk managers as opposed to European risk managers," says Lawson.

And the market for senior risk managers is likely to remain good for the remainder of the year. "As we enter the pay review and bonus period, we expect to see more senior moves which is likely to open up more opportunities at the director/managing director level, so it is a good time to be looking for a new opportunity if you are a risk management professional," says Lawson.

James Sayer, director, risk and compliance at recruitment company Pure Search, says that "there is always a good demand for risk professionals", but he adds that "it depends if the right vacancy is there for the right candidate at the right time."

For example, the financial services sector is always a good industry for risk management professionals as these roles are always in demand from junior to senior level, says Sayer. However, he adds that some of these roles can be on a short-term contract or interim basis to help the organisation plug a specific skills gap quickly.

Insurance strong

Simon Caplan, chief operating officer at Arthur, a specialist insurance market recruitment agency, says that there is a strong market at present for risk managers in the insurance industry, particularly at junior levels (such as risk analysts) where annual salaries can range from between £30,000 and £60,000.

"Risk management functions in the insurance sector have become top heavy over the past few years, a possible consequence of major projects such as Solvency II. Now that the majority of the work for Solvency II has been completed and we move to an embedding phase, insurers are looking for more junior-level risk experts and there appears to be a shortage," he says.

> "Insurers are looking for more junior-level risk experts and there appears to be a shortage

However, demand to fill junior positions may be outstripping supply. According to Caplan, those new to the profession may be unwilling to move to another employer so quickly after starting. "Junior risk professionals are less likely to move jobs because the role they currently have is their first job in risk management," he says.

There are other reasons why junior risk managers are reluctant to jump ship. "They have a keenness to build up their sector experience, capabilities and skill-sets with their current employer, and this overrides the draw for more money elsewhere," says Caplan. "They don't necessarily have the personal and professional confidence either, and they haven't had enough career experience to become less risk averse and see the potential benefits in risk."

Experts say that employers are looking more closely at specific skills-sets that candidates might have. Lawson says that quantitative skills are in high demand, with employers looking to review models and risk engines based on regulatory change, such as the fundamental review of the trading book (FRTB) – already being dubbed "Basel IV" because of its risk versus capital requirements – and changes to the International Financial Reporting Standards. "We have seen an increase in recruitment activity across credit risk management which was a quieter risk discipline last year. This activity has been particularly noticed at the vice-president level within non-banking financial institutions' credit risk analysis," says Lawson.

Cyber risk

Cyber risk and security, technology risk and data privacy have also all been areas of increased demand and are likely to continue to be busy throughout 2017, says Lawson. "We have seen a shift from hiring in operational risk at the second line to the first line, with many firms looking to hire embedded control specialists within the business now that most have well-established three lines of defence frameworks," he says.

However, other recruiters say that their clients are not looking for specific cyber risk management skills from the people they want to hire. For example, Sayer believes that clients largely consider cyber risk skills to be the remit of the IT department rather than risk management. He also says that "experience is the key issue that companies are looking for", adding that "the right set of skills is more important than qualifications alone."

"Cyber risk management skills are not something that insurance clients have been specifically requesting in risk management profiles," says Caplan. "However, chief risk officers and risk managers will have to become tech-savvy moving forward as cyber risks are increasing as vulnerabilities are found internally in the company and externally in the policies they are writing."

Instead, employers are looking for trained risk managers and solid risk management experience, as well as commercial nous. "A risk professional who can demonstrate good commercial sense, as well as an understanding of how the business works in the way they design, develop and embed risk management, will find him or herself on the wish list for profiles our clients are looking to hire," says Caplan.

He adds: "On top of that, they want people who can communicate to the board and use risk management as a tool to drive the business and detect opportunities as well as risks. Having these attributes, combined with the ability to hit the ground running and being familiar with the how the role works already, will top the wish list."

Some employers are also being more specific about the professional background, qualifications, experience and skills that they want the candidates to have. "If a client wants someone to work on a particular regulatory or compliance issue, then the client will only take someone on who has that experience already – they don't want to train them on the job," says Sayer.

"It is also apparent that clients are looking for risk managers who are also business advisors and can help with business strategy as well as risk and compliance. Furthermore, they want their risk professionals to have business acumen, strategic awareness and good presentation skills," he adds.

While the level of experience may be the key issue that employers are looking for, Lawson believes that professional risk qualifications are useful – so long as they match what the client specifically wants. "It depends on what type of risk manager you are looking to hire. Generally, we find that experience is the focus above qualifications, but there are specific areas where qualifications become more relevant," he says.

"For example, a chief information security officer (CISO) qualification is highly sought after for security officers, as is a certificate in quantitative finance (CQF) for quantitative risk managers. Qualifications like those that the IRM provides would definitely strengthen a profile for a risk manager," Lawson says. With such a buoyant recruitment market, those with the right mix of qualifications, skills and experience could make 2017 a career-defining period.

Neil Hodge is a freelance journalist.

> **Chief risk officers and risk managers will have to become tech-savvy moving forward as cyber risks are increasing**

IRM QUALIFICATIONS

The IRM has several qualifications that can prepare risk management professionals for a range of roles across different industries. Internationally-recognised and made up of various distance-learning modules that can be completed with six to nine months (at most), the IRM courses include the Certificate in Risk Management in Financial Services, the International Certificate in Enterprise Risk Management, and the International Diploma in Risk Management. The IRM also provides short cyber risk management training courses (see weblink for more details: https://www.theirm.org/training/all-courses.aspx).

Drone wars

As commercial drone use begins to take off, new devices are coming onto the market that could bring them back down

BY SARA KAMIYA

On 7th December 2016, Richard B took delivery of an Amazon Fire TV and a bag of popcorn. From placing the order on Amazon's UK site to receiving the goods took 13 minutes. And they were delivered by a drone from Amazon's Prime Air fulfilment centre.

The business' trial currently involves just two shoppers who live within a few miles of the company's drone base near Cambridge. Over time, Amazon plans to expand this programme to include few dozen — and later hundreds — of customers who live in the area. The drones can carry packages weighing up to 2.6kg.

Amazon says that the current batch of customers will be able to order seven days a week, but only during daylight hours and when the weather is okay to fly. Cambridgeshire is ideal for the trial because regulations usually require the drone operator to have a clear line of sight to the craft. Flying over unpopulated fields seems to have satisfied the Civil Aviation Authority (CAA) when it visited the site in summer 2015.

Lawyers say regulations in the UK are generally favourable to companies wanting to experiment with autonomous aircraft, but there are restrictions. Amazon can test drones that fly beyond line-of-sight in rural and suburban areas; flights where one person operates multiple, largely autonomous drones; and sensor performance associated with sense-and-avoid technology.

> There have been several cases of people shooting down drones that have flown over their homes because of privacy fears

Image credit: DroneShield

> The laws are lagging behind the technology

Commercial organisations must get clearance from the CAA, which has also published a simple *Dronecode* for hobbyists.

Minefield

By contrast, the US is a legal minefield for commercial organisations hoping to take advantage of this potentially revolutionary delivery service. Companies need to register the drone and apply for clearance to the Federal Aviation Administrator (FAA), which includes passing background checks for security purposes. But individual states are passing their own separate laws and ordinances on drone use. In Oklahoma, for example, the state banned drones from flying over critical infrastructure facilities – such as oil refineries and gas stations.

"The laws are lagging behind the technology," Lisa Ellman, a partner at Hogan Lovells in Washington, DC, told *Global Insights* magazine. "At the moment, because of these restrictions, companies have to separately apply for exemptions to the rules. It would be better if innovators and policymakers could work together on the rules."

The reason for such nervousness is the risk of injury to people or damage to property. Reports of possible drone sightings to FAA air traffic facilities increased to 1,274 between February and September 2016, according to the latest figures available from the FAA, compared with 874 for the same period in 2015. Pilots reported them colliding with their planes.

Not verified

But the FAA said: "Although the data contain several reports of pilots claiming drone strikes on their aircraft, to date the FAA has not verified any collision between a civil aircraft and a civil drone. Every investigation has found the reported collisions were either birds, impact with other items such as wires and posts, or structural failure not related to colliding with an unmanned aircraft."

While businesses such as Amazon are working hard to comply with this complex patchwork of regulations, their unmanned airbourne vehicles are coming under fire – literally. There have been several cases of people shooting down drones that have flown over their homes because of privacy fears. Although it is illegal in the US to discharge firearms in a populated area, or to willfully damage another's property, no successful prosecutions have yet been brought.

But new products are coming onto the market that could be game changers. The DroneDefender rifle by Battelle and the Dronegun by the US-Australian company Droneshield can take a drone out of the sky without damage. Both use signal jamming to effectively take control of the device, after which the gun's operator can land it safely. Dronegun has a range of 2km. Theiss has made the Excipio Net Drone Gun, which is itself a drone that fires a net onto the target vehicle to bring it down.

While these products have obvious security and risk mitigation uses, as commercial drone flight increases, they could also become attractive to criminals. Whether businesses will respond by developing anti-capture features to their own drones, only time will tell. ER

Institute of Risk Management

A perfect fit

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

RESILIENT RELATIONSHIPS

Sign up for our free, upcoming IRM/ SAI webinar: *Building resilient relationships – how to handle third party risk effectively.*

With growing geo-political, environmental and financial uncertainty, businesses must build resilient relationships with their suppliers, customers and stakeholders. But with more customers and businesses using and adopting open technology platforms, the nature of those relationships is transforming.

The webinar will explore how to build resilient relationships in this changing world. Key discussion points include what key risks are on your radar today? What are the main challenges to developing resilient 3rd party relationships? How can technology be used intelligently to help manage these risks? How can risk managers deal with disruptions and threats?

Panellists include Mark Boult, a Director for DNV GL. Charles Low, SAI's head of business development for risk across EMEA. Raza Sadiq, risk management at Covéa Insurance and Chairman of the IRM's Special Interest Group (SIG) in ERM in Banking and Financial Services. Clive Thompson, a senior projects Director in Willis Towers Watson and *Enterprise risk* editor Arthur Piper.

The webinar takes place: 23 March 2017 at 14:30 GMT. Register today: http://bit.ly/2m65j0U

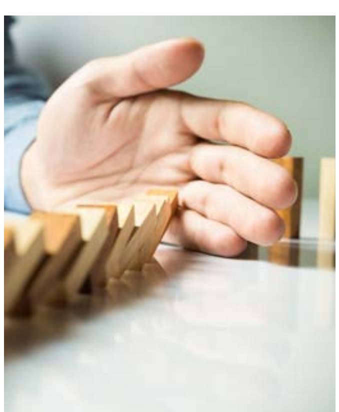
LEARNING FROM FAILURE

Why do transformation initiatives and global businesses experience significant losses or even fail despite large investments? Even with some of the brightest brains in the sector leading projects for organisations, it's an uphill struggle resulting in failure to meet the objectives.

Media coverage and regulatory fines have little impact on organisations who don't seem to learn from the events that led up to the failures. Instead of looking to change the culture of the business, organisations repeat these mistakes time and again with some business leaders leading from the bottom up.

The seminar will explore recent events to examine the underlying causes of failure in business; look at the common and repetitive effect of these causes; and to discuss the role risk management plays in the success and failure of business. This will be followed by a panel discussion with thought leaders to explore the strategic position of risk management to the success of businesses.

Risk perspectives series: causes and effects of risk management's failure in organisations, 21st April 2017, 14:00 – 16:00. IRM London office. Member price £55. To find out more visit: http://bit.ly/2n3rtVt



MEMBER SCOOPS MINING AWARD

IRM trainer Dr Sarah Gordon has been recognised as one of the top 100 mining women in the world by Mining Global magazine. Gordon is chief executive officer and founder of Satarla, a risk management consultancy based in London and Johannesburg. As CEO, she oversees the company's risk management tools, which are utilised in several sectors, including mining.

Prior to starting Satarla in 2004, she worked with Anglo American in the UK, Brazil and South Africa. Sarah has an undergraduate degree in Earth Sciences at the University of Glasgow and a PhD in the composition of primitive meteorites.

RISK AGENDA

As part of the IRM's 30th Anniversary celebrations, it has embarked on a major research project into the future of risk – *Risk agenda in 2025.* IRM welcomes on board its technology sponsor Sword Active Risk.

IRM is launching a membership survey on the future of risk in April and the interim findings will be presented by IRM Chair, Nicola Crawford, at the Active Risk Manager Global Conference on 22 June at London's landmark Dorchester Hotel on Park Lane.

Attendance is free for IRM members, visit: http://www.armgcc.com/ to book your place today. Check the website for details of the regional roadshows. The final report will be presented to IRM's Risk Leaders Conference in November 2017.

FUNDING TOP CHARITY RISK

Risk managers ranked funding stability as their number one risk in a snap poll of members by the IRM's charities' special interest group. Financial stability came a close second, with general fundraising issues coming third. Health, safety and security ranked fourth, with organisational resilience and continuity coming fifth.

The top risks survey reflects the views of 125 respondents. The group intends to use the results to inform its programme of work for 2017. For more information on the group: http://bit.ly/2lHIHIR

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

Leaders in Forensic Investigation

Hawkins
Leaders in forensic investigation

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

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

Risk and audit management software solutions

Symbiant are one of the world's leading providers of Risk and Audit management software. The solution is designed for collaboration and comes as a complete suite which can be separated in to Audit or Risk sets. Symbiant is designed for non Risk / Audit specialists to use, simple and intuitive but with a lot of back end flexibility and automated functions. CIO magazine have rated Symbiant as one of the top 20 risk solutions in the World. They have off the shelf or custom solutions to fit all budgets and requirements. Install on your own infrastructure or SaaS. 30 day free trial.

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

Risk, insurance and safety technology solutions

Ventiv Technology is the preeminent provider of global risk, insurance, and safety technology solutions. Working in partnership with our clients to understand their challenges and key business objectives, our solutions adapt to your precise needs and evolve with you. Providing a central platform to work across your company and functions to eliminate silos and help embed risk management. Delivered with Ventiv's extensive risk management and technology experience to provide unsurpassed client value and operational excellence. Winner of 2016 IRM Risk Management Solution of the Year.

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

Risk management information systems

NTT DATA Figtree Systems is a specialist software provider for risk management Information Systems. Figtree Systems is used globally for incident and OH&S management, claims management, corporate insurance and employee benefits management, fleet and asset management and enterprise risk management. By using system features such as workflow automation, document management and creation, reports and dashboards, smartphone and web-based data-capture and email notifications, users have reported increased productivity, lowered costs and improve risk management processes. Easily configurable, the system is available in the traditional client-server model as well as a Software as a Service (SaaS) model from ISO 27001 compliant datacentres.

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

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

Risk management software

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

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

Risk management software

Origami Risk is the industry's #1 Risk Management Information System (RMIS) as ranked by the 2016 RMIS Review. Founded by industry veterans committed to bringing new ideas and advanced features to the RMIS market, Origami Risk's innovative software is designed with the latest technology and a focus on performance and ease-of-use. It features powerful workflow, advanced reporting and analysis tools, and intuitive features to improve productivity and better manage Total Cost of Risk—saving our clients time and money and enabling them to be more successful. Learn more at www.origamirisk.com.

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

Risk management software

Xactium is a cloud based Risk Management software vendor that is changing the way regulated organisations evaluate and manage their risk. Our aim is to enable risk and compliance managers to transform the value of risk management within their organisation, through the use of modern, agile and collaborative software. Our risk management platform ensures that organisations such the FCA, Direct Line Group, HS2 and HomeServe can stay up to date and respond rapidly to both business and regulatory change.

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

Flaky news

There seems no end to the debunking of fake news, but what about the poor reporting of questionable evidence?

It's a mediated world. Risk managers rely on a wide range of news, research, internal and external data to build up as accurate a picture of reality as possible. Very little of this information is experienced directly – empirically verified – so it depends on a filtering process involving a wide range of people. That requires both trust and scepticism.

A recent article on *Enterprise Risk* website wrote about how fake news could come from seemingly reliable media outlets. Fake news is a form of story that is not true, but widely debated. But a new storm has blown up in the science community about flaky news – reporting that just isn't accurate.

"The unfortunate fact is that much of science reporting is a morass of ideologically driven junk science, hyped research, or thick, technical jargon that almost no one can understand," wrote Tom Hartsfield and Ross Pomeroy, editors of the science news portal RealClearScience, which instigated the research. "So, whose science news should you trust?"

The editors teamed up with the consumer advocacy American Council on Science and Health (ACSH) to produce an infographic showing the best and worst science news outlets. The research asked: is the science content compelling enough to read? and, is the coverage driven mostly by evidence? Top ranking publications included the dedicated science journals *Nature* and *Science*, the business weekly, the *Economist*, and the alpha-geek magazine *Ars Technica*.

ACSH's Alex Berezow, who collaborated on the research, has a dim view of journalism in general, science journalism in particular: "Not only is it susceptible to the same sorts of biases that afflict regular journalism," he says, "but it is uniquely vulnerable to outrageous sensationalism. Every week, it seems, an everyday food is either going to cure cancer or kill us all."

> In a world of proliferating messages and voices, the louder you shout, the more likely you are to be heard

Sensational stuff. But risk managers will recognise that last statement as an indictment of risk reporting in the media, as much as one of science journalism itself. The journalists, it seems, are careless with both their use of scientific evidence and risk evaluation. Or are they?

While the editors at *Nature* were flattered to be ranked first, they were not impressed. "The judges' criterion of evidence-based news is arguably problematic," they wrote. "Many journalists could reasonably point to the reproducibility crisis in some scientific fields and ask — as funders and critics are increasingly asking — just how reliable some of that evidence truly is."

While mainstream science reporters typically depend on peer review as the official stamp of approval from the research community, that may no longer be adequate. "Many scientists would complain (even if only among themselves) that some published studies, especially those that draw press attention, are themselves vulnerable to bias and sensationalism," *Nature* concluded.

So, not only is the news story flaky, but some of the evidence that it depends on is inherently weak. The reasons for these faults, though, seem connected. In a world of proliferating messages and voices, the louder you shout, the more likely you are to be heard. If some experts are not above pepping up the evidence to further their careers, it spells trouble for everyone interested in evidence-based research.

Risk managers facing such a confusing media landscape need to beef up their critical skills. They also need to make sure their own reporting is as sound and as clear as possible. In today's febrile media world, flaky risk management is the last thing that's needed.


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