Enterprise Risk

Autumn 2020 / www.enterpriseriskmag.com

The official magazine of the Institute of Risk Management

Realities of ransom: Tata Tea's ordeal / **Serious play:** cyber scenarios for boards / **Spotlight on Zimbabwe:** education and awareness / **Changing perspectives:** why diversity matters / **Upping the ante:** IRM's revised Diploma

Rewriting the economic rulebook: the pandemic is radically reshaping the rules of the global economic system

IRM's revised International Diploma in Risk Management

Advance your career with the global benchmark qualification in Enterprise Risk Management

About the International Diploma in Risk Management

For 30 years, IRM's International Diploma in Risk Management has been the global choice of qualification with risk professionals and their employers. The IRM has revised the syllabus for the International Diploma to ensure our students are informed of the best practices in risk management. Students will benefit from our new online learning platform, the Virtual Learning Environment (VLE). The VLE supports students step-by-step through the modules and provides activities and quizzes to help master the subject matter. Students can submit their assignments when they are ready, no more exam centres.

Benefits of the International Diploma

- Gold standard in ERM qualifications
- Global recognition
- Master's level equivalent qualification
- GradIRM designation with option to apply for CMIRM
- Designed to ensure you are current and competent

What's new about the International Diploma

- Students can enrol at any time
- Learn from anywhere in the world via the VLE
- Access the learning platform via PC, tablet or mobile phone
- Assessed through practical work-based assignments that can be submitted online at any time
- Quicker (provisional) results on marked assignments
- Potentially shorter study time more suited to those who are working

What our students say

Helen Hunter-Jones, CMIRM
Chief Risk Officer, Pay.UK, United Kingdom
"I took the International Diploma in Risk Management and could not have got to the position I have without it. The IRM can provide access to many other practitioners and help build your professional network."

Find out more at:

www.theirm.org/diploma-mag

Resilience, risk and recovery

irm

Developing risk professionals

Enterprise Risk

Autumn 2020

Editor
Arthur Piper

Produced by
Smith de Wint
Cobden Place, 5 Cobden Chambers
Pelham Street, Nottingham, NG1 2ED
Tel: +44 (0)115 958 2024
risk@sdw.co.uk
www.sdw.co.uk

Sponsorship and Advertising Sales Manager
Redactive Media
IRMsales@redactive.co.uk
Tel: +44(0)20 7324 2753

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

ISSN 2397-8848

About the IRM
The IRM is the leading professional body for Enterprise Risk Management (ERM). We drive excellence in managing risk to ensure organisations are ready for the opportunities and threats of the future. We do this by providing internationally recognised qualifications and training, publishing research and guidance, and setting professional standards.

For over 30 years our qualifications have been the global choice of qualification for risk professionals and their employers. We are a not-for-profit body, with members working in all industries, in all risk disciplines and in all sectors around the world.

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

Anger over algorithms

As the world is desperately trying to get back to normal, new problems keep cropping up. Plans are going wrong every day. For instance, the UK government's attempts to build a moderating algorithm to account for a potential disparity between teacher assessment grades for their pupils' achievements and the more objective measure provided by exams ran into opposition – and was eventually abandoned.

These things happen during difficult times. The narrative around the problem, however, should give businesses food for thought. Ministers were concerned primarily with grade inflation – the idea that if too many people achieve the highest marks, the exams are devalued.

This has not been a problem recently. In 2019, 25.2 per cent of UK entries were awarded an A or A* grade; in 2007 it was 25.3 per cent. In 2020, it was 27.6 per cent, according to Ofqual, the exams regulator. Compare a potentially one-off rise of 2.4 per cent in people achieving the highest grades with around 40 per cent of all students – especially those from state-run schools – having their grades lowered by the algorithm. While it is true that some students will have gained an advantage by not sitting exams, that pales into insignificance compared with those losing out through the moderating program.

> **The public debate turned into an issue of people (teachers and students) versus machines (the algorithm)**

I think there are two useful lessons to learn from this issue. By far the most common complaint about the fairness of the moderated results was that they had been decided by an algorithm. As readers of this magazine will know, an algorithm is just people's choices disguised as a computer program. The public debate turned into an issue of people (teachers and students) versus machines (the algorithm).

As the effects of the pandemic continue, businesses are increasingly digitalising their processes. Any unfairness – perceived or actual – that gets baked into the system will be greatly amplified by technology. And greatly resented if the way that decisions are made is not transparent and well explained prior to them coming into effect. Risk managers should strongly encourage role-playing the effects of any such sensitive, automated decision-making processes on large data sets prior to making the system live.

The second lesson is that organisations need to fully understand their risk appetite around reputation. How much flak can the directors take before having to reverse the decisions they make? In that respect, politicians are lucky. General elections come around only once in five years. But customers can go overnight to competitor organisations.

Sometimes, it may be better to let a few people get away with an easier time than accidentally punish many more unfairly while trying to close a loophole.

Arthur Piper
Editor

Risk Management – Illumination or Infoxication

Infoxication: A phenomenon related to the development of the Internet which refers to the difficulty or impossibility of taking a decision or keeping informed about a particular subject due to the endless amount of data and content that exists on the web or in electronic systems.

BY REBECCA COPE-LEWIS

Today, with risk systems or an Excel spreadsheet we can gather and report on a plethora of information. We can generate analytics on risks to objectives, risk interconnectivity, changes in cost exposure over time and much more.

This is all great, but are we asking too much of the front line (the people who are capturing all this data), and are we as risk managers too enthusiastic in capitalising on the opportunities that risk data can offer us? Are we putting our own risk management frameworks at risk of being less than effective? How much data do we really need to help us make sound risk-based decisions to enable us to meet our objectives?

Choices and mandates

Frameworks allow people to operate in a consistent manner but must have a fluidity to them, so they are effective and allow a degree of flex in the approach while still achieving the desired outcome.

So why, when it comes to spreadsheets and systems, do we suddenly become rigid and fixated on the need to complete every field just because it is there? And why do we develop the need to make people segregate each risk into five levels of Work Breakdown Structures, when three could suffice?

Just because you can does not mean you should, and it could negatively affect the entire "risk experience" of our colleagues – and that is definitely not one of our key objectives.

Why do invasive neurosurgery when a CAT scan is sufficient to expose and diagnose the problem? Our front-line people are not meant to be neurosurgeons and they do not need a multitude of reports showing them their risk data in various guises to make decisions on what to do next. If we want them to manage their risks, we must make sure that what we ask of them and what we provide is appropriate for them to make *their* decisions.

There is a balance between gathering data that you can use to make decisions and data that is collected because your system allows it. Collecting too little data could result in the inability to produce SMART risk management plans. Too much data may be overwhelming and could conversely result in actually collecting less or poorer-quality data, creating a perfunctory mitigation plan.

Devil in the detail

Being a risk manager myself, I recognise that sometimes the devil is in the detail. Capturing additional information may not be considered 'relevant' at the front line. But it is important for correlating risk information or trying to understand the wider risk picture. It's a balancing act.

"How much data do we really need to help us make sound risk-based decisions to enable us to meet our objectives?

So, we must always ask ourselves "How much data do we really need?" to answer the relevant questions, and "Could we reach the same conclusion or plan with less?".

Risks are sometimes hard to qualify and/or quantify, and as it is the role of our front-line people to provide the data on which we rely, we should make it as easy and relevant for them as possible.

There is an art to risk management, but it should not be a mystic art. Let us not be seduced by system or spreadsheet capability, but use it wisely to help illuminate and not to obfuscate.

Rebecca Cope-Lewis, DipQ MCQI, CQP, CIRM, is head of enterprise risk management at riskHive Software Solutions Ltd. www.riskhive.com

Contents

Autumn 2020

10

16

22

26

30

Material weaknesses: impact, prevention, and technology

BY TIM LE MARE

You've likely heard the phrase "shouting 'fire' in a crowded theatre".

For all you pub quiz aficionados, it was coined by Supreme Court Justice Oliver Wendell Holmes Jr during an early 20th-century case. The saying roughly translates to causing panic by words or actions.

For risk professionals, there's no greater panic than having to declare to senior management and the board that a key risk has materialised into a material weakness. The mere whiff of the possibility of a material weakness in a company's annual report – the "fire in a theatre" – is enough to cause panic.

And, that's not to mention the powerful reaction it stirs up in shareholders.

Finding the link

To see what impact material weaknesses can have, we looked at the performance of all the companies on the New York Stock Exchange and Nasdaq Stock Market, and then contrasted that performance against any material weaknesses, deficiencies or disclosures incurred that year.

The results were harsh. Companies that reported a material weakness in 2019 experienced a 12-month average drop of 19 per cent in share price. In a 2019 study, KPMG analysed annual filings released by SEC-registered public companies between November 2014 and May 2019.

Three key takeaways from their report:

• Of the 731 companies that filed a report between 2014 and 2018, almost a third disclosed material weaknesses in multiple years

• Common reasons why material weaknesses occurred were IT, software, security and access issues; inadequate control design; and segregation of duties

• From 2017 to 2018, the study noted a 12 per cent increase (from 28 per cent to 40 per cent) of material weaknesses with IT, software, security and access issues at their root

How to protect yourself (or recover)

If your company has experienced (or fears) a misstatement or weakness, here are actionable steps you should be considering:

• **Review your risk assessment process:** An effective risk assessment process is key to reducing the likelihood and impact of a material weakness. Reflecting on how others have been impacted by a material weakness can help refocus your risk assessment process and help ensure you don't make the same mistakes

• **Drive collaboration:** In our increasingly complex organisations, pulling in a wide network of colleagues to collaborate in the risk process is paramount, particularly to avoid complacency and groupthink

• **Understand your data:** Since there is no "Department of Connect the Dots" in an organisation, risk managers need to have a firm understanding of the data available to drive the risk process. Key to this is supplementing qualitative risk assessments with high-quality quantitative risk data

> **For risk professionals, there's no greater panic than having to declare to senior management and the board that a key risk has materialised into a material weakness**

• **Use of technology:** Invest in technology that permits line of sight across the organisation's risk, control and assurance landscape. Having disconnected processes means issues fall between the gaps. If your organisation struggles to have a shared view across risk, control and assurance, then it's worth exploring how integrated risk technology can help address this.

KPMG's report notes that the technology teams use – or don't use – frequently plays a part in their ability to avoid material weaknesses. When you infuse stronger technology into your risk, control and assurance process, you enable your entire team to work more efficiently, and teams get unparalleled visibility into the process and the data within. Clarity means control, and control means eliminating unwanted surprises.

Workiva's research in this area proves that investors see material weaknesses as a "fire in a theatre". For the risk firefighters in your organisation, the best extinguisher in your arsenal is technology.

Tim Le Mare is regional sales director, integrated risk, at Workiva. To find out more about how Workiva can help, get in touch with the team today.
Workiva.com/uk | info@workiva.com | +44 203 868 0550

Upping the ante

IRM has relaunched its flagship qualification to make it easier to study and more relevant to everyday business life

IRM's Diploma was introduced in 1986 and has since then set the gold standard of quality for qualifications in risk management. It has given thousands of students worldwide a robust and comprehensive grounding in both academic and practical risk management learning. Today it is a fundamental part of obtaining Certified Risk Professional (CMIRM and CFIRM) status, demonstrating sound professional knowledge to employers and clients.

Over the years the qualification has been updated and adapted several times in response to a changing world. Our latest update has significantly enhanced the qualification to help risk professionals better serve their organisations in these difficult times. We have also taken the opportunity to redesign and improve the student experience, deploying today's best practice in educational delivery and assessment methods.

The basics

Students come to the Diploma generally when they have taken IRM's International Certificate in Enterprise Risk Management, found it interesting and useful, and want to move on to gain further knowledge and a higher-level qualification. The Certificate is the gateway qualification to the Diploma – modules 1 and 2 of the Certificate form modules 1 and 2 of the Diploma, providing a seamless transition to the higher qualification. The Diploma adds a further four modules, including an extended work-based practical project.

The Diploma and the Certificate have always been primarily delivered though distance learning, with study guides and essential reading materials provided to students with further support from Module Coaches and the Student Team at IRM. At the end of the study period, students would sit examinations in exam centres near to their places of work or home.

The new approach brings our delivery up to date with enhanced online study support and assessment methods. First, all content is now managed online through a specialist education portal, called Moodle, used by many schools and universities in the UK, giving it more academic rigour as well as enhanced convenience and ease of access. Second, Diploma exams have been replaced by practical assignments that are relevant to risk management as it is practised in the real world, assessed by our team of professional examiners.

Reflecting the new, more flexible structure, students can now enrol anytime during the year and can study and complete their assignments from anywhere in the world. Study material is easily available via computer, tablet or mobile phone, making learning on the go simple. Students also receive quicker (provisional) results on their marked assignments, rather than having to wait three months following the exams.

> **Our latest update has significantly enhanced the qualification to help risk professionals better serve their organisations in these difficult times**

Future proof

Completing the Diploma provides you with an academically robust Master's level equivalent qualification. Successful Diploma students receive first their GradIRM designation. We hope that many will choose to go further and apply for the CMIRM designation, giving them Certified Risk Professional status, after the qualifying period (three years' of practical experience) and then potentially move on to Fellowship (CFIRM) if they have the ultimate designation in their sights.

Study time is potentially shorter than the previous exam route as students had to wait for the study and exam dates. Now students have more freedom when and how to study, which is more suited to those who are improving their prospects while working full-time.

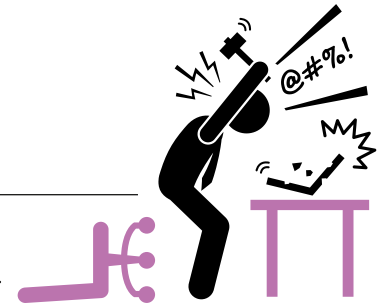
Taken together, these changes will enable risk professionals worldwide to better match their study schedules with their working lives, as well as emphasising the practical application of the deep risk management knowledge in the course. And students can enrol now at any time of the year – so there is no longer any need to wait.

For further information contact our student support team on studentqueries@theirm.org or on +44(0)2077099808. Carolyn Williams is IRM Director of Corporate Relations.

Trending

DATA

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



The difficulties of working from home

Which of the following are the most significant challenges associated with increasing the population of employees working from home at your organisation?

27%
Making sure that all remote employee computing devices have been securely configured

26%
Giving remote employees secure access to the corporate network

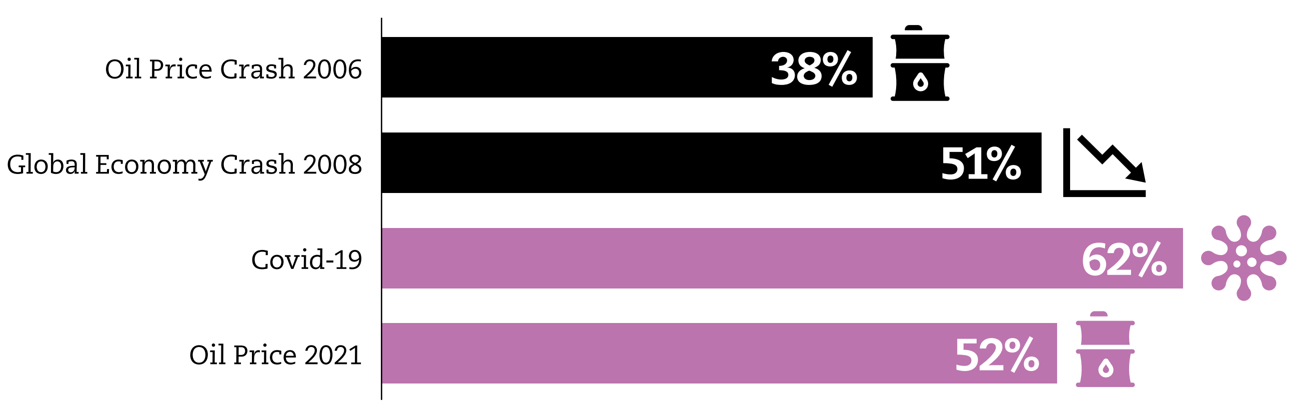
24%
Monitoring traffic and user behavior associated with remote employees

23%
Coordinating moves, adds, and changes with IT/network operations

Source: The impact of the Covid-19 pandemic on cybersecurity, ESG research report.

Energy sector faces two of its biggest challenges

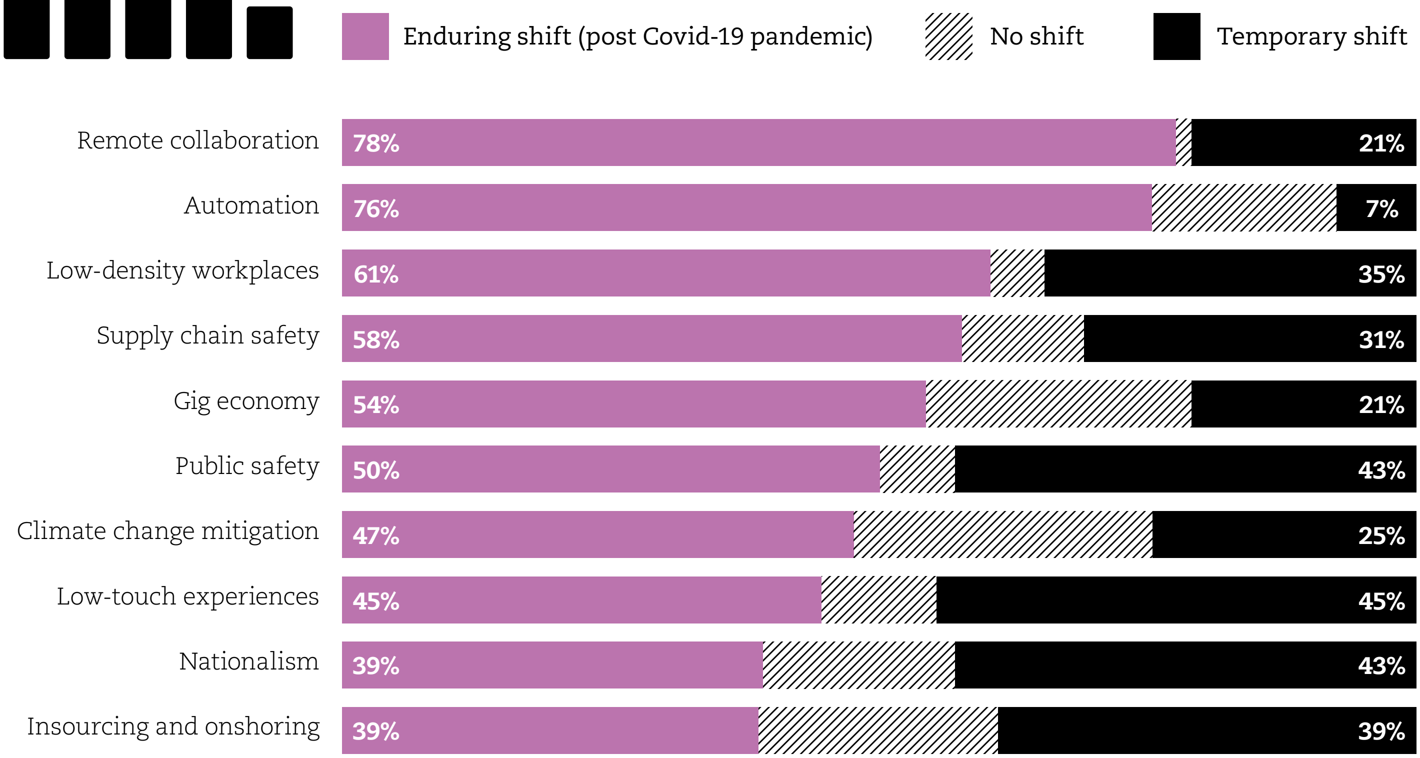
How do the following events compare in terms of impact on your organisation?



Source: IRM Energy SIG energy global industry survey, May 2020, published August 2020 in Disruption, uncertainty and the role of risk management, IRM. For a extended report, see page 35 of this issue.

CEOs’ predictions for post-Covid world

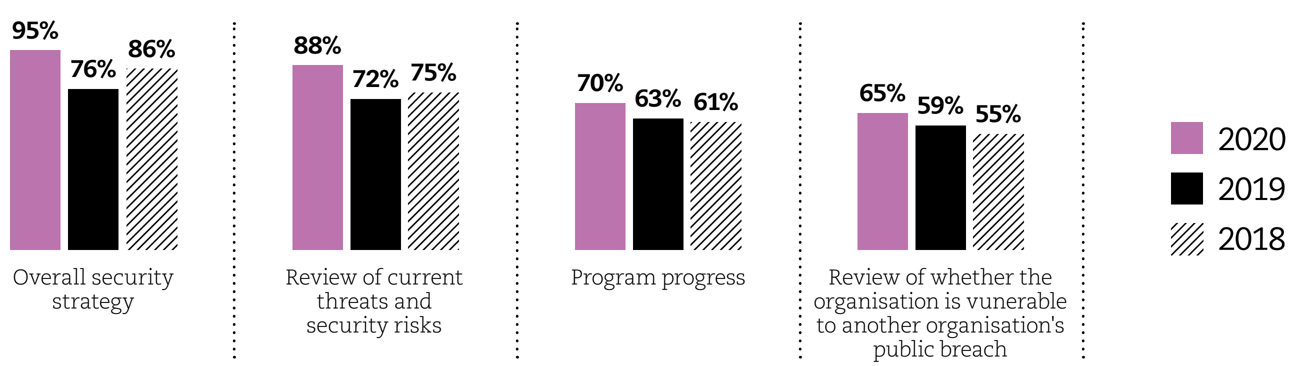
Remote working, automation and low density workplaces here to stay



Source: CEO Panel Survey, How business can emerge stronger, PWC.

Boards getting serious on cyber

Top cybersecurity areas of interest for board/management identified by survey respondents



Source: Reshaping the cybersecurity landscape, Deloitte-FS-ISAC

Rewriting the economic rulebook

The pandemic is radically reshaping the rules of the global economic system. Risk professionals will need to work smarter to help boards navigate unpredictable risks and take new opportunities quickly as they arise

BY TEJ PARIKH

The COVID-19 pandemic has shone a light on vulnerabilities that were growing in the global economic system for decades. The rapid rise in the cross-border flow of trade, people, money and ideas has been facilitated by ever-growing complexity, efficiency and interdependence. Car components are forged across continents, elaborate financial instruments are used to gain or hedge exposures to international developments and hyper-lean production lines deliver customised products to buyers thousands of miles away – in just a matter of days.

In any normal state of the world, that is a supreme vehicle for profit, growth and innovation, which has even shown its resilience amid geopolitical flareups and natural disasters. But when global tail risks do occur, they can trigger a domino effect that can crash the entire system, and even send it into reverse. The 2008 financial crisis was the first such warning sign that global contagion risks ought to be accounted for. Banks have now been encouraged to hold more capital and conduct regular stress-tests, while regulators have sharpened their tools and oversight. With COVID-19, business leaders will need to do similar.

> **The 2008 financial crisis was the first warning sign that global contagion risks ought to be accounted for**

Global economic disruption

The pandemic has brought global disruption on a scale not seen since the Second World War. The International Monetary Fund expects the Great Lockdown to shrink the global economy by around 5 per cent over 2020. That dwarfs the 0.1 per cent annual contraction at the time of the global financial crisis. Indeed, the impact of the pandemic is far more wide-reaching than the banking crisis. Now, advanced economies and emerging markets are both in a tumble, whereas breakneck growth in China and lofty commodity prices provided some fallback for the latter in 2008.

In developed nations, alongside weak consumer confidence, the scars of unemployment and corporate indebtedness, incurred during the trough, has dispelled any notion of a "v-shaped" recovery. Many advanced economies are not expected to return to pre-COVID-19 activity levels at least until the end of 2021. In emerging markets, debts have grown as money has been dished out by governments and central banks to stave off defaults and currency runs, leaving many on a precipice. The emergence of a global consumer class will also be set back with World Bank estimates suggesting at least 70 million could be pushed into extreme poverty.

All this is before any potential new waves of COVID-19 are even factored in. For boardrooms of international businesses, it paints a particularly challenging picture. The World Trade Organization estimates that global trade could fall by up to a third in 2020, with almost all regions suffering double-digit declines in trade volumes. Supply chains will continue to face snags as demand

> **Even as economies begin the long road to recovery from the lockdown period, uncertainty alone will likely keep a rein on business activity**

> Anti-globalist sentiments may gain more sympathy, and some governments may be driven toward protectionism, raising tariffs and protecting strategic industrial players

Image credit: Gwoeii / Shutterstock.com

remains patchy and businesses attempt to adjust to the new risk environment by rebuilding stocks and reducing regional exposures. Investor appetite will also dry up, as growth prospects remain unclear. The United Nations estimates a 30 to 40 per cent contraction in global foreign direct investment flows, with the steepest cuts expected in the transport, hospitality and manufacturing industries. Tapping into the international workforce will also be complicated by ongoing travel restrictions.

Certain uncertainty

Even as economies begin the long road to recovery from the lockdown period, uncertainty alone will likely keep a rein on business activity. The global Economic Policy Uncertainty Index, which aggregates sentiment on the economy through newspapers, reached its highest during the pandemic. It remains above peaks reached following 9/11 and the 2008 financial crisis. The most pressing uncertainty for firms is the prospect of further outbreaks, lengthening the downturn. New waves have been evident in many major economies, including Australia, China and Germany. So far, a rise in cases has been largely handled with localised actions, limiting economic damage. While nations have now built up more experience, and resources, to handle a rise in infections, businesses and investors will remain wary of a return to lockdowns.

If a vaccine is found, it may take considerable time before it is in use universally. Meanwhile, the damage incurred over lockdowns will also add to uncertainties about the domino effects it may trigger. Risk specialists surveyed by the World Economic Forum rank a surge in bankruptcies, among both large firms and SMEs, alongside a prolonged recession as the most worrisome risks for business. Last year, corporate debt had already reached record levels in China and the US. With businesses across the globe turning to government loan schemes and other bridging finance, recoveries will be hampered by interest repayments, and interconnected production chains will remain vulnerable to contagion if key businesses struggle to stay afloat.

Geopolitical risk

Countries will face similar challenges, raising uncertainty for global business operations. Emerging markets will remain vulnerable to low commodity prices and depreciating currencies as debts mount. Significant social unrest is also likely given potential increases in poverty, unemployment and inequality. Meanwhile, as public debt in advanced economies balloons to 122 per cent of GDP this year, it may hold back governments' ability to support firms' recovery. Indeed, national responses to the crisis will also affect firms. Austere measures may cut growth prospects, while populist policies may drive profligacy.

It likely that anti-globalist

> “In a global economy liable to change and particularly with so much uncertainty in official forecasts, firms will need to embed a culture that regularly monitors risks, updates compliance procedures and adjusts business models to fit the dynamic climate

sentiments may gain more sympathy, and some governments may be driven toward protectionism, raising tariffs and protecting strategic industrial players. This dynamic was already playing out between the US, Europe and Australia, in relation to China. And regardless of who is in the White House come the end of 2020, a focus on domestic challenges and economic nationalism across the world will limit any momentum behind a multilateral approach to global growth. For businesses operating in multiple jurisdictions, this heightens the risk of tax, trade and regulatory barriers emerging on cross-border operations. Domestic governments may even be more sceptical of foreign enterprise, with potential implications for merger and acquisition activity, visa eligibility, technological collaboration and data flow.

The new abnormal

It is clear the pandemic has exposed a powder keg of knock-on exposures that are now at risk of being ignited. With so many complex and dependent moving parts, it will become even harder for businesses to react to changes in the new global economic risk landscape. Evaluating the vulnerabilities and building a risk register will be the first step, as firms with an international footprint will need to get to grips with potential pressure points in their business. Market, supplier, staffing and geographical exposures will all need to be looked at with extra suspicion. Going the extra mile to obtain in-depth and accurate market intelligence will be a differentiator. With the rapid news cycle and ever-growing sources for global analysis, the need to be even more discerning with information will be important. Special risk-monitoring working groups, across business lines, could help avoid internal blind spots and ensure all departmental perspectives are taken into consideration.

A clear mapping of exposures, and understanding of their potential implications, will be a crucial base for many firms in understanding where to build resilience. The growth, trading and regulatory assumptions underpinning just how global economic and political dynamics might impact those vulnerabilities will then need to be stress-tested. More frequent engagement with boards in a time of heightened risk could be important to ensure strategic plans are fresh and the results of stress-tests are well understood across the organisation. Boards should also play an important role in the horizon-scanning necessary to build out various scenarios to test finances, alongside challenging management teams more generally on contingency planning and operational resilience.

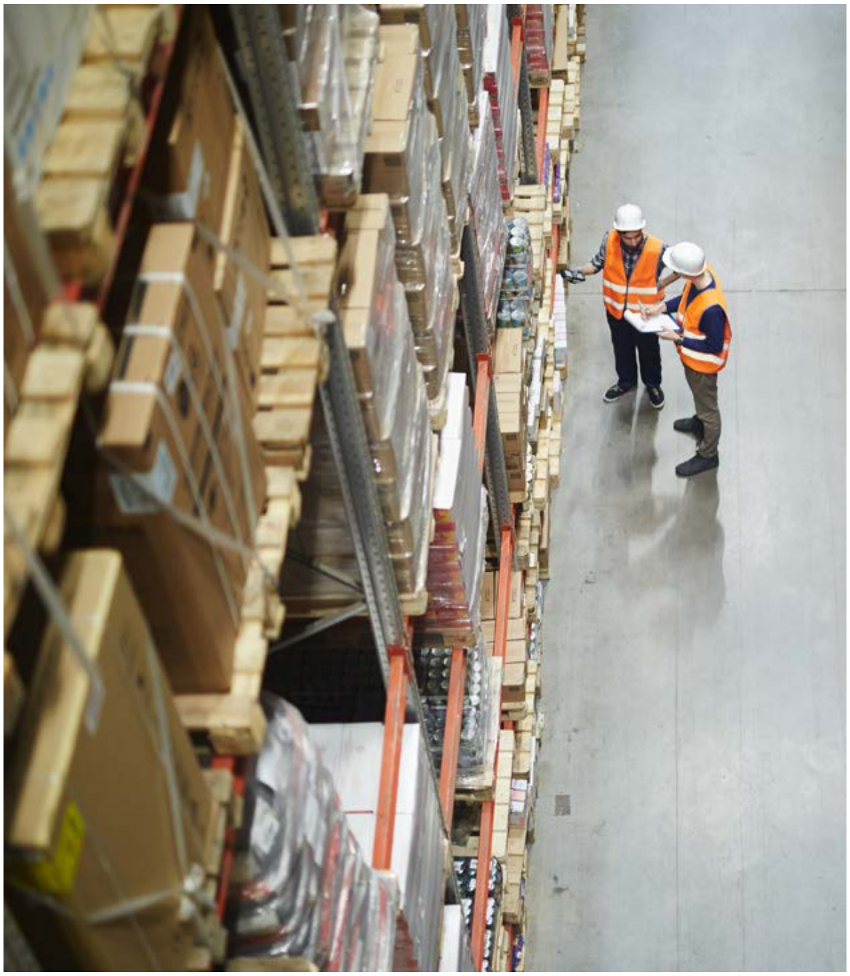
Firms will need to understand just how their organisations may look in “all bets are off” scenarios. What may happen if expenditures double, or entire markets became inaccessible, or key product regulations change? With the pandemic shattering many existing assumptions on what is possible, businesses may consider it sensible to assume the ongoing health and economic dynamics precipitated by the virus will continue to leave many outside-the-box scenarios on the table for the time being at least. This modelling should help determine the shape of the business plan and necessary financial reserves for the year ahead – and it should kick-start discussions for continuity arrangements and plans Bs should worst-case scenarios come true.

Above all, in a global economy

HOW RISK MANAGERS CAN BUILD RESILIENCE

1. **Map exposures:** Assess potential pressure points across your entire business including key markets, supply chains, and sources of finance. Consider how economic, political, and regulatory shifts may directly impact your own operations, as well as your suppliers and customers.
2. **Stress test:** Understand what “business as unusual” looks like for your organisation. Assess how scenarios of interrelated risks impact your bottom line, and how mitigation strategies perform even in extreme and one-off events. Hope for the best, prepare for the worst.
3. **Build resilience:** Boost reserves, diversify, and do not neglect the “just in case” mindset. In a time of complex interconnected risks, incorporating some slack into your business processes can be an asset. Understand just how much wiggle-room your organisation may need.
4. **Be agile:** Invest in expertise, technology, and networks to always ready your organisation for the next transformation. Insights on your risk footprint, real-time data on your operations, and a broad range of business relationships can keep your organization one step ahead.
5. **Constant horizon scanning:** Embed a culture of continuous strategic oversight, risk auditing, and red teaming across your organisation. Be wary that the playing field may evolve before you have even got your original “play” through.

liable to change and particularly with so much uncertainty in official forecasts, firms will need to embed a culture that regularly monitors risks, updates compliance procedures and adjusts business models to fit the dynamic climate. Strong communication will be essential to this. The success of rapid business transformations will rely on how well managers and key staff are kept in the loop and aware of evolving responsibilities. This will hinge on effective leadership that keeps an eye on future developments, with a view to adapting the business model today. Throughout it all, technology will be crucial. Real-time business data, enterprise risk management systems and productivity-enhancing ICT will play an important role in spotting and diagnosing pressure points.



Just in time vs Just in case

For many global firms, the new risk environment will ultimately see a shift from a "just in time" mindset to one of "just in case". Where low inventories and specialised production chains fostered end-to-end supply chain efficiency, firms may now want to build in more slack and generate long-term resilience. This may mean holding more stock should shipping operations jam up again, reducing the complexity of supply chains, and diversifying suppliers and labour forces, even at a cost, to hedge against potential tariff and visa restriction changes. With the precise size of downside risks complicated by several intersecting factors, businesses may not see resilience as an inefficiency, but as a necessary short-term speed bump to support long-term competitiveness. No doubt, investors will also be wary of fragile business models.

> **Just as businesses will need to engage more frequently in strategic oversight to mitigate risks, unearthing opportunities will become all the more important – and lucrative**

But just as businesses will need to engage more frequently in strategic oversight to mitigate risks, unearthing opportunities will become all the more important – and lucrative. Less-trodden geographies – such as eastern Europe and the Balkans – may become more popular for European-headquartered businesses as they seek to spread risk from more extensive global value chains. With the fiscal purse-strings loosened, policymakers will also be eager to stimulate business investment to drive economies forward, which could support R&D, technology and green opportunities. More generally, with the pandemic itself reinforcing a trend toward digital platforms and working from home, global businesses will need to keep their fingers on the pulse of rapidly evolving consumer trends, which will dictate market entry and new product decisions.

The pandemic presents a challenge like no other for business leaders. The global economic system has received a sharp jolt, and there is little clarity on when and where it will land. Disruption is here to stay. Businesses risk losing more than 40% of annual profits once a decade in a complex global economy threatened by trade wars, cyber attacks, pandemics, and climate change, according to Mckinsey. The firms that will succeed will constantly be on their toes, building long-term resilience and strategic risk management into all processes. Indeed, it is the directors that work on their business, and not just in their business, that will thrive.

Tej Parikh is chief economist at the Institute of Directors. @tejparikh90

The realities of ransom risk

Kidnapping is likely to increase as the world tips into recession. Tata Tea discovered that balancing political risks, employee wellbeing and business ethics is an important but difficult path to take

BY SHASHANK SHAH AND HERSH SHAH

Rising uncertainties impacting individuals, organisations and countries across the globe has created a lot of negativity and animosity within and between communities. The fight for opportunities is likely to continue with only so much up for grabs, particularly in certain parts of the world.

This situation makes organisations vulnerable to security risks, and these need to be taken very seriously considering the duty of care they owe to their employees. In fact, India and Brazil feature in the top 20 countries for kidnap, extortion and illegal detention risks. A total of 100,555 (23,814 male and 76,741 female) victims were reported kidnapped or abducted in 2017, according to the latest figures from the US Overseas Security Advisory Council. Of these, 56,622 (14,296 male and 42,326 female) victims were children and 43,933 (9,518 male and 34,415 female) were adults.

There are numerous root causes to a kidnap and ransom risk, be it an assumption of wealth on the part of the employee and their company, or political and ideological reasonings. Generally, however, the number-one goal on the minds of kidnappers is money.

A post-COVID world is no exception to this situation

> **Previous health crises have indicated a rise in kidnap for ransom and other criminal activity especially after an outbreak as severe as COVID-19**

especially with a large number of employees already losing their jobs. Previous health crises have indicated a rise in kidnap for ransom and other criminal activity especially after an outbreak as severe as COVID-19. There was an average 45-50 per cent increase in unemployment (as well as a massive increase in criminal activity) in Ebola-affected areas, such as Liberia and Sierra Leone in 2014, for example. But, as this case study shows, the causes that create the conditions for kidnapping and the way that businesses and governments respond is complex and changes over time.

Tata Tea

After three decades in various capacities as a TAS officer, Krishna Kumar became the managing director of Tata Tea in 1991. It was the time when militancy had started gaining the upper hand in Assam where the company had several tea plantations. The United Liberation Front of Assam (ULFA) had gained control over the southern banks of the River Brahmaputra, while the northern banks were under the command of the National Democratic Front of Bodoland (NDFB) militants. The militants demanded what was called "protection taxes" per kg of tea produced and per hectare of land owned.

The ULFA was an indirect outcome of the mass movement of 1979 by Assamese students and government servants for the detection and deportation of illegal migrants from Bangladesh. It took six years and loss of several hundred lives before the Assam Accord was signed in the presence of Prime Minister Rajiv Gandhi on 14 August 1985 with the

> **"Tata Tea's policy was not to buy protection but to earn it through the company's goodwill with employees and the local community**

Image credit: OlegD / Shutterstock.com

> **Tata explained they would not be able to pay any protection money. Instead, they would willingly undertake work like building hospitals, providing jobs to locals and extending medical support**

explicit declaration that all foreigners who had illegally entered Assam on or after March 25, 1971 (formation of Bangladesh) would be deported. However, it took three decades before any concrete action was taken on the ground during which period the militant and insurgency movements in Assam peaked.

Kumar observed that most tea companies were paying protection money, which collectively amounted to over ₹100 crores a year – about $14 million. It was common knowledge that big companies had been earlier forced to pay fringe groups to ensure safety in disturbed states like Punjab, Kashmir and West Bengal. The Tatas refused to pay, even though one of their employees, Dr Scaria, was killed by the militants in Nalbari in March 1990. Darbari Seth, then chairman of Tata Tea, had maintained that Tata Tea's policy was not to buy protection but to earn it through the company's goodwill with employees and the local community. This approach did work in the company's favour until April 1993 when Bolin Bordoloi, a Tata Tea manager and the youngest son of Assam's first chief minister, Gopinath Bordoloi, was kidnapped from Guwahati. The Bodo militants demanded a ransom of roughly $7 million (₹54 crores using today's current exchange rates).

"We went from pillar to post pleading for support. I went to Mother Teresa, Kanchi Shankaracharya and even met the prime minister, Narasimha Rao, to get support. While we got moral support, there was limited help," said Kumar. The company decided not to risk the lives of 175 managers working across the Assam valley. They were living like prisoners in the estates with the Assam Tea Protection Force shielding them. The company called all the managers to Kolkata and shared with them the company's inability to pay the militants. Conscious of the danger the managers and their families faced, Tata Tea proposed to pay them their full salary and pension if they opted to retire and withdraw from Assam. The company urged them to return to their native places. "Interestingly, not one manager responded to that. They all said that they would stand by their duty," said Kumar.

Investment

In the meanwhile, the Bodos gradually reduced the ransom for Bordoloi from ₹54 crores to ₹5 lakhs (about $7,000), the amount they had spent on keeping him in captivity. The Tatas did not even agree to that. However, they agreed to greater investments for the wellbeing of the Bodo community. Tata Tea was already managing 63 hospitals, 280 adult literacy centres, 173 childcare centres and 110 schools in the region. When Bordoloi was released after 11 months, Tata Tea helped set up a 65-bed referral hospital at Chabua in the heart of Bodoland at an expense of ₹7 crores. When everyone thought that peace was finally achieved, it turned out that it was too good to last.

In 1995, following the example of Bodo militants, ULFA started demanding money from Tata Tea. ULFA chief Paresh Baruah wrote a letter to Kumar demanding 100 walkie-talkie sets. "There was no question of buying and supplying military equipment, the value of which was about ₹8-10 lakhs. This was an ethical issue. Firstly, it was a supply to militants. Secondly, it meant resorting to illegal means for doing it," he said.

The company met and communicated all details to the Assam government. However, most of the information was supposedly leaked from the secretariat of the chief minister, Hiteswar Saikia. One late night, Kumar received a call from someone who claimed to be Baruah himself. He said that he had all the information that the Tatas were giving the government and threatened him. The Tatas now decided to go to the Intelligence Bureau (IB) of the

> **"Would you react by taking a soft option or would you take a hard decision based on ethics?**

Image credit: Mazur Travel / Shutterstock.com

> Tata Tea managers were even arrested for ‘waging war against the state’

REDUCING THE RISK OF KIDNAPPING

- Detailed due diligence and review of kidnap and ransom risks in the region before setting up operations
- Communication and education to employees working in high-risk regions will equip them with basic skills required to manage such situations
- Avoid too much social media activity at individual and company level in the high-risk region
- Ensure employees are not carrying high-value items and are dressed in simple attire at all times
- Build relationships with local authorities, police officers and government and set up a crisis management process including raising of a trigger
- Conduct a mock “ransom drill” like a fire drill to be better prepared for situations and train employees
- Insurance companies offer kidnap and ransom insurance, a crime coverage that protects organisations against potential financial losses that arise during an extortion or illegal kidnap.

central government, the agency entrusted with matters pertaining to national security. Kumar and his colleagues met the IB’s additional director several times. Every meeting was followed by letters to them, which were on record. The IB advised two things: don’t pay the militants in cash or kind; continue the dialogue with them, else they will retaliate.

Dialogue and arrest

Tata representatives met with ULFA representatives in different places including Bangkok and explained to them that as per the Tata code, they would not be able to pay any protection money. Instead, they would willingly undertake work like building hospitals, providing jobs to locals and extending medical support. Consequently, a medical aid scheme was introduced and funded by the Tatas through which any Assamese could apply for hospitalisation within and outside the state. The IB was kept in the loop throughout.

A year into this scheme, one of the patients, whose name was registered as Bonti Baruah and was treated for a pregnancy-related blood disorder in Bombay, was found to be Pranati Deka, ULFA’s culture secretary. She, her baby and accomplices were arrested at Mumbai airport. The Prafulla Kumar Mahanta-led Assam government, who had not been kept in the loop due to past experience of information leakage, was furious and alleged collusion between the Tatas and the ULFA, and that the former was funding the latter – a charge of sedition.

SS Dogra and Brojen Gogoi, Tata Tea managers, were even arrested for “waging war against the state”. The news hit national headlines – the Tatas were charged with treason. The matter went to the High Court and eventually to the Supreme Court, which observed that the Tatas had approached the highest security agencies of the country, the police and the Home Ministry and provided all supporting documents while engaging with the

Image credit: IDREES ABBAS / Shutterstock.com

> The Assam government considered the Tatas' medical scheme a conspiracy to support militants

militants. They could not be funding the ULFA and were not guilty.

"It is such a paradox that on one hand we had been charged with sedition by the authorities in power at that time, and on the other hand we had been directed and guided by the highest national security agency of the government of India," Kumar said in a subsequent interview. "We didn't disclose this publicly because we had 175 members of the Tata family across the Assam valley. And to disclose that would have been putting their lives at risk. So, we decided not to do that and went through those nine months of gruelling challenges,' he recalled in an interview several years later.

A difficult path

The Tatas acted on the belief that the security agencies would communicate with the state government, an assumption considered naïve by observers in an era of coalition politics. While the Assam government considered the Tatas' medical scheme a conspiracy to support militants, to many in Assam the real problem was the unflinching Tata principle of not paying.

Yet, this was an example of how a lot of trouble could have been avoided by just paying a small amount of money. When there were large companies that had officially declared ransom payments, denouncing the Tatas' actions as seditious just because they continued to engage with the militants on the advice of intelligence agencies smacked of a political witch-hunt.

Several industry observers considered the Tatas' decision pragmatic – balancing business obligations with employee safety and fulfilment of social objectives for the local Assamese populace. Had the Tatas decided to exit from Assam, it would have had a serious impact on the local economy and affected the livelihoods of 20,000 labourers who worked in its 21 tea gardens. "This is an example of how moral questions become issues when you run a company. Would you react by taking a soft option or would you take a hard decision based on ethics? The Tatas have taken this stance several times. It is part of our philosophy. It influences every decision we take," said Kumar.

While local circumstances will always play a decisive role in how risk managers guide their organisations in such situations, some general guidelines can be useful for mitigating such risks (see *Reducing the risk of kidnapping*). Even so, organisations always face a conflict choosing between payment of ransom for protecting employees versus being ethical and disassociating from such practices. ER

Dr Shashank Shah has been a SAI Fellow at Harvard University and is a strategic advisory board member at IRM India. Hersh Shah is the Chief Executive Officer of the India Affiliate of IRM and also Chair of IRM's Regional Group in India. Part of this feature originally appeared in *The Tata Group: From Torchbearers To Trailblazers (Penguin Random House, 2018)* authored by Dr. Shashank Shah, and is reproduced with permission from the publisher.

Serious play

Convincing boards to focus on cyber security is no easy task. Two role-playing scenarios at a recent IRM event offer valuable lessons to risk management teams. Readers can try the scenarios for themselves

BY DANIEL ROBERTS

From TalkTalk in the UK to the American retail giant Target, and from Saudi's Aramco to the UK's National Health Service, we've seen and will continue to see attacks on companies' computer systems with the objectives of stealing customer or commercial data, or disabling or destroying computer systems and data, or plain financial extortion. The 2017 WannaCry cyber-attack on the NHS was estimated to cost that organisation £92 million. The 2012 attack on Aramco targeted over 30,000 computers. The number of attacks is increasing, and there is little we can do to reduce their likelihood.

And for all this time, the constant refrain has been, "How can get boards to take this seriously?" Convincing boards to focus on cyber security is no easy task, when those working in the business have competing priorities, responsibilities and rewards structures. Risk professionals play a key role in communicating with the board and demonstrating why cyber security matters and requires board attention.

The existence of these conflicting priorities within an enterprise will result in key individuals taking various stances to cyber security mitigations: they may be supporters, indifferent or be blockers with

> Risk managers play a key role in communicating with the board and demonstrating why cyber security matters

(valid) reasons to focus on issues other than cyber. Understanding context and motivation is vital.

Expectations

Boards see their primary focus as being on strategic risks. They expect management to deal with operational risks. Cyber security is a classic strategic risk masquerading as an operational risk. As the examples in the first paragraph show, unmitigated cyber risk can have huge strategic impacts. Unfortunately, the expectation that management will deal with operational risks can distract board attention from the strategic risk that cyber represents to the business.

Therefore, in order to convince the board to focus on cyber security and the cyber threat, both management and the board need to be convinced that cyber security is not just an operational risk. Risk management has an important role in providing the contextual data and information that demonstrates the potential magnitude of the cyber threat to the viability of the enterprise.

Recently a meeting of the CRSA (Control Risk Self-Assessment) forum in London, hosted at the IRM's offices, addressed this very issue. One session focused on two role-plays designed to highlight the challenges that management (operational to the C-Suite) face, and the conflicting operational risks that can lead to a de-prioritisation, or even ignoring, of cyber. Neither case represents a real company or actual situation, and the session was held under the Chatham House Rule – but many participants said they had experienced similar situations.

For the two scenarios, one

> “Cyber security is a classic strategic risk masquerading as an operational risk

was at the operational level and highlighted the conflicting priorities within a project. The second dealt with the trade-offs and decisions that senior executives could face. In each scenario, individual priorities acted to de-incentivise escalation of cyber from the operational to the strategic level of risk.

Complex project choices

The first scenario looked at a project with issues and delivery concerns leading to a situation in which information security measures, while acknowledged as critical, were actually "kicked into the long grass" by each group that considered the case. The premise was fairly simple: the project is in its final stages but has run over budget and over time, and the user community's level of frustration is rising to breaking point.

The role-play highlighted the competing constraints facing any business when it comes to systems implementation. The various strains on all members of a project team, including the leadership, sponsor, and steering committee, require the balancing of resources and priorities. Sometimes individual incentives end up outweighing the broader needs of the business.

The groups were then asked, each playing a specific role, to provide a recommendation, as a group. As expected, not one of the groups said that project implementation should be delayed until security concerns were addressed. In one group, the person playing the role of the IT infrastructure representative threatened to "call in internal audit". The response was, "So you plan to stab your colleagues in the back?"

The final takeaway for participants was that it will be difficult to gain the internal allies if such support will be counter to their own needs, responsibilities and rewards.

C-Suite and external expectations

Likewise, at the C-Suite level, internal and external expectations can be such that investment in cyber security becomes a secondary consideration behind meeting the short-term demands of shareholders, markets or owners. This second role-play set out to demonstrate the push and pull of competing requirements, again against a backdrop of

> **"In the two role-plays, as in real life, there were too many competing priorities**

systems implementation coupled with quarterly reporting needs, in challenging market conditions.

The four participants (the chief operating officer (COO), chief financial officer (CFO), chief information officer (CIO) and director of communications) each have competing priorities, yet all are keenly interested in ensuring company success.

Again, each group had difficulty abandoning their roles' self-interest, though they all recommended that the CIO push cyber security to the top of his or her agenda for the coming quarter. Only one group overcame the conflicting priorities to recommend that the business "take the hit" this quarter and focus on cyber security, while also communicating to the markets that they were doing so to improve the

HOW WOULD YOUR ORGANISATION PERFORM?

Role-play 1: Complex project choices

A new system is in the final stages of development and should go live in three months. Testing is ongoing with the usual bugs and use-case mistakes. The project expects (for the third month in a role) to come in at exactly 109 per cent of budget, thus avoiding the need to request additional board authorisation. The COO has committed to the board that the system will go in on schedule. IT infrastructure reported that the servers will be ready but that they will not be within the secured domains used by other corporate systems, and admitted that it might be possible, under "extreme" circumstances, for a hacker to gain access to "some" data.

Imagine the meeting (via Zoom or Teams of course) to discuss the situation, where the primary participants are:

1. **Project manager**. Bonuses are at stake, as well as future projects. Worse, you are in regular steering committee meetings with the sponsor (and team). They are becoming a nightmare of complaints about timing and diversion of resources for testing.
2. **IT infrastructure**. He or she knows that the 4-month re-architecting estimate is probably optimistic. A few people in the IT team know too much about your systems, hoard that information, and honestly, would have been "moved on" if they didn't hoard their knowledge. Can you trust them to fix the architecture on time or budget?
3. The **Operations Manager** is concerned, as users have been crying out for this system for years, budgets have been cut, headcount reduced, and people are reaching breaking point. Meanwhile, the project continues to demand more of your frontline experts for "testing".
4. **Strategic planning**. Your models show that this system is going to boost profit by 5 per cent annually, with an immediate 2 per cent this year, to a profit line that is already stressed. Missing the targets is not an option, as the markets have priced in an earnings forecast that has improved numbers "baked in".

Try this role-play and see what you would agree to recommend to the board. Whose interests gain priority and why?

HOW WOULD YOUR ORGANISATION PERFORM? CONTINUED...

Role-play 2: Shareholder expectations

Shareholder expectations include the meeting of targets, primarily revenue and profitability targets, that ensure either a dividend flow (private companies and utilities) or sustained growth in share price. Senior managers, "C-Suite" executives and directors know this and know that their bonuses and futures depend on a track record of delivering to shareholders' expectations.

Welcome to the Pre-Executive Committee (Exco) video call as they prepare for the upcoming earnings release season. Things seem to be on track, and the second quarter results were in line with COVID-19 revised expectations. This quarter, however, could be a little more difficult. Trading conditions are worrying the marketing director, while internal costs are not dropping as quickly as budgeted. The new system is going to be at least two months late, possibly three, pushing benefits into the fourth quarter, or possibly next year.

Participants have some difficult decisions to make:

1. The **COO** has numbers to make, promises to keep, regardless of COVID-19, which has hit every company, not just us. The numbers received from senior managers are promising, but "I've seen numbers like these before, and they are always overly optimistic."
2. **Director of corporate communications** has a team well versed in the motto of "Bad news is good news; good news is no news". He or she is worried because they feel things are reaching a point of stretching credulity.
3. The **CFO** has managed to, just, get the numbers right for the first quarter and second quarter results, but this quarter will take a small miracle to reach even the publicly released new targets. Missing targets in a pandemic is excusable, but missed revised targets may severely limit the longevity of a CFO. The numbers expected by the markets (or owners) are possible, but there had better not be any down-side surprises.
4. The **CIO** knows that infrastructure is only barely supporting the users, but InfoSec is saying that a serious architecture review is needed (again, "review" means they know there are problems), and the company simply cannot continue to avoid significant new investment. Your proposals for security investments themselves will increase the overall IT budget to the equivalent of 11 per cent of revenue from the current 10 per cent of revenue, a level that is already at the high end of the scale for this kind of business.

Imagine the conversation that will take place. What would you be recommending the CEO says in the next earning call / shareholders' meeting? Why would you make those recommendations?

company's ability to protect and service customers in the future.

Summing up:

In the two role-plays, as in real life, there were too many competing priorities. But there is hope in each, in that the need was recognised, and there are ways out, albeit not "this quarter".

In both cases, the role of risk management has not been highlighted. Why? Because risk management was not "at the table" for the discussion. Yet risk managers have the role and opportunity to influence everyone at the table and an obligation to ensure that no matter what is said at the operating level, the board is considering strategic risks. Risk management can provide the prompts for the board to ask questions beyond what is in the board pack and can ensure that such questions lead to cyber threats and cyber security being included in an upcoming board pack.

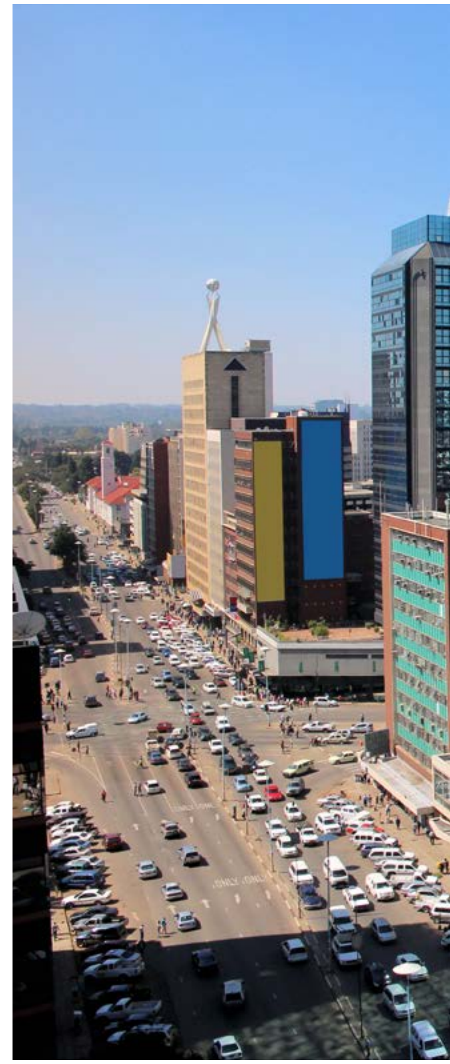
Convincing the board to focus on cyber security also requires gaining management's focus on the same problem. The board can act unilaterally in requesting information, but if management understands the threat as well, realistic and actionable recommendations can be prepared and provided to the board. Top-down meets bottom-up. The first step to gaining board focus is to gain management's focus. That requires the reframing of cyber threats as a strategic and not an operational risk. ER

The full report of the CRSA meeting can be found here: https://www.theirm.org/news/cyber-security-and-directors-report/

Daniel Roberts is a board level risk advisor and director of the consultancy GRMSi. https://bit.ly/2GpTWjr. Contact: daniel.roberts@grmsi.com

> **If management understands the threat as well, realistic and actionable recommendations can be prepared and provided to the board**

Spotlight on Zimbabwe's risk profession



Education and awareness are key to developing the risk management profession in Zimbabwe, according to a ground-breaking IRM-backed study

BY SMARNTHA SHONHIWA & DAVID CHIMSITU

In an ever-dynamic world, risk management plays an important role in ensuring that organisations continue to generate value for their stakeholders and shareholders. Our baseline risk management survey (supported by IRM) was the first of its kind in Zimbabwe, and it covered risk management personnel drawn from four sectors of the economy: financial services, mining, tourism and energy. These sectors are considered to be some of the major drivers of economic turnaround in Zimbabwe with the mining sector being the biggest foreign currency earner.

The purpose of the risk management survey was to understand how these sectors are approaching risk management. Additionally, the level of risk management development, training, and impediments to the development of risk management within the targeted sectors was also gauged. We hope that the results obtained from the survey will form the basis for more focused researches within the targeted sectors. This is vital in promoting the growth of risk management within sectors, improving the process of value creation and ultimately aiding the turnaround of the Zimbabwean economy.

> **The level of professional risk management education and training is one of the most important indicators of both current and potential future growth of the risk management profession**

> The financial services sector is leading in the development of risk management legislation

Professional risk management

The level of professional risk management education and training is one of the most important indicators of both current and potential future growth of the risk management profession within the sectors targeted by the research. We enquired from the research participants whether they had any professional risk management training, the institutions from which they obtained their professional qualifications, the relevancy of the qualifications to their day-to-day work, and the general challenges that they face obtaining professional qualifications.

Only 25 per cent of the research participants had professional risk management qualifications. These professionals were from the tourism and financial services sector. The results show that the uptake of risk management as a profession is still very low in the sectors that participated in the research.

The main reason given for the low uptake of professional risk management education and training is the high cost involved in pursuing professional qualifications. This is further compounded by a lack of recognition of the professional qualifications by some of the employers within the sectors targeted by the research. However, based on the risk management legislation and regulatory trajectory, most sectors will soon recognise risk management as a standalone office for each organisation.

The office of chief risk officer and chief compliance officer are increasingly becoming common in response to regulatory developments. The main challenge, however, with the early stages of the regulatory development is an overemphasis on workplace health and safety, especially in the areas of mining and energy. Currently, the financial services sector is leading in the development of risk management legislation.

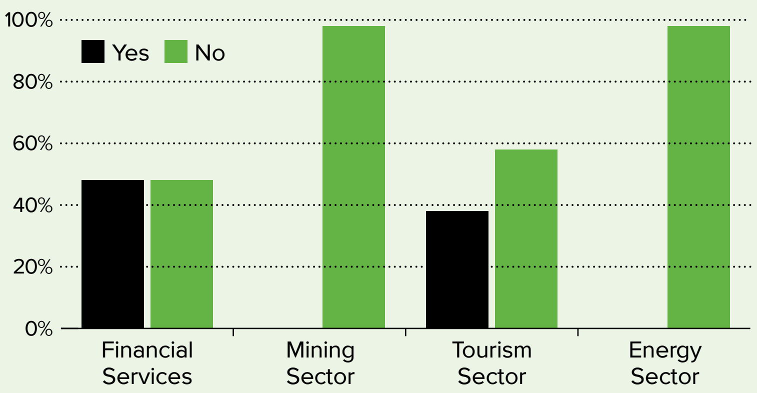
Research participants with professional qualifications agreed that knowledge gained from obtaining those qualifications was relevant to their risk management work. The sources of information that led the participants to eventually join the different professional risk management societies/institutions include: personal research, recommendations from friends, and recommendations by the Insurance Institute of Zimbabwe. However, personal research was the most common source of information for the research participants.

Challenges

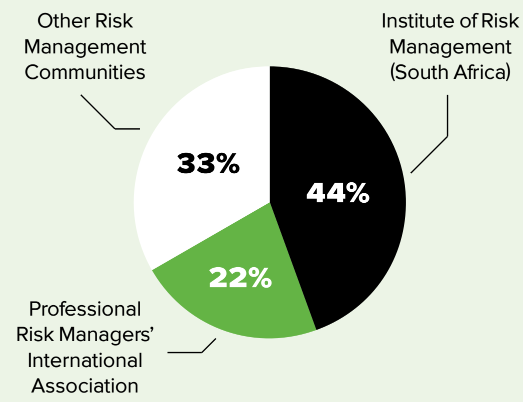
The top challenges currently bedevilling risk management professionals in Zimbabwe include trust issues, problems in monitoring and managing risks, inappropriate use of risk matrix, mismeasurement of known risks, cultural problems, lack of commitment and, last but not least, lack of training (see *Top risk management challenges in Zimbabwe*). These challenges cut across all the four sectors participating in the research. However, the views and opinions regarding the extent to which each of the above challenges affects the research participants was largely dependent on the sector and level of employment.

Sectorial differences in the views regarding the problems of risk management point out the differences in the level of development of

RISK MANAGEMENT PROFESSIONAL QUALIFICATIONS BY ECONOMIC SECTOR



WHICH INSTITUTION, SOCIETY OR COMMUNITY?



> **A common comment from all the sectors was that appointed risk management officers were often disconnected from the risk situation on the ground**

risk management as a discipline within each sector. Problems of risk identification were more prevalent in the financial services and tourism sectors, while problems of trust were most prevalent in the mining and energy sectors. An interesting result was that legislation did not pose any challenges to risk management on all the four sectors represented in the research. We found this to be an important result since legislation provides impetus for growth and development. However, it is also important to highlight the differences that exist in the level of development of legislation by economic sector.

Participants from the financial services sector were drawn from insurance and insurance-related companies, banks and investment companies. The regulation within this particular economic sector is leaning towards risk-based regulations. Whilst this regulatory trend is still in its infancy, it is an easy prediction that players within the financial services sector will eventually adopt a holistic approach to risk management. Thus, companies within this economic sector will be required to implement Enterprise Risk Management systems.

Participants from the energy and mining sectors were drawn from the local power utility companies (Zimbabwe Electricity Transmission & Distribution Company and Zimbabwe Power Company), fuelling and gas stations, and gold mining companies, respectively. The respective regulators for these sectors impose stiff penalties on companies that do not follow minimum risk management practices. However, the scope of the definition of what constitutes risk management is still limited within this economic sector. The current emphasis of regulations is on adequate management of safety, health, environmental and quality risks (mostly workplace-related risks) arising from the operations of companies within the sector.

Participants from the tourism sector were drawn from the Zimbabwe Tourism Authority (ZTA), hotels and related companies in hospitality. The industry seem not to have any particular penalties for lack of implementation of risk management systems by the regulator, but the need for companies to be approved by travel and holiday destination agents implies that at a minimum, companies must implement international risk management best practices on hotel management and tourism.

Planning

Differences in the views and opinions of risk management challenges by the level of employment show the subtle problem of communication and approach to risk management. Generally, the weightings given to certain challenges by senior management and executives were different from those given by entry-level management and non-managerial staff.

An observation from the research showed that most of the risk management planning is done at board level while the implementation is done by entry-level managers and non-managerial staff. Thus, a common comment from all the sectors was that appointed risk management officers (if they existed at the organisation) were often disconnected from the risk situation on the ground. This observation was most prevalent in the energy sector where the non-managerial staff were mostly not sure what role the risk management officers play within their organisation.

Besides these top risk management challenges, the additional risk management challenges affecting all the four sectors represented in the research were: volatile economic environment, lack of proper education on the importance of risk management, limited human resources and a disconnect between the risk officers/ risk management department and the rest of the organisation.

Policies and frameworks

Research participants were asked questions on the existence of risk management policies; drivers of the development of risk management where responsibility for development and review of risk management policies lie; the frequency of policy reviews; and effectiveness of the risk management policies at their organisation.

We hardly came across any organisation that did not have one form of risk management policy or another in place. All the research participants indicated that their organisations have risk management policies. However, the differentiator between organisations and economic sectors is the extent to which the policies are implemented. Legislation is the main driver of the development of risk management at organisational level in all the four sectors that participated in the research. Thus, the initial view when developing risk management policies is that of the need for compliance to avoid penalties and other sanctions that may be imposed by the regulators. Besides regulation, the other emerging drivers of the development of risk management include the need to cut costs, loss minimisation, continuity planning and adoption of international best practices.

The responsibility for risk management lies mostly with the risk management department in all the four sectors of the economy. Responses on the effectiveness of risk management policies varied from one organisation to the next. The most common reasons given for lack of effectiveness of risk management policies were lack of proper implementation or lack of risk management resources.

Annual inspections and audits are the most common control methods used to ensure compliance and adherence to risk management policies. Additionally, research participants indicated that internal and external penalties could be imposed for non-compliance with risk management policies and standards.

The most commonly used tools for risk management include risk transfer and risk retention. Insurance and subcontracting were given as the most used methods of risk transfer. Companies in the mining and energy sectors also indicated that they sometimes create or rent insurance captives to manage their big risks.

Raising awareness

Based on the results obtained from the baseline survey we concluded that there is a need for increased awareness on the importance of risk management and risk management training opportunities in all the four sectors that participated in the research. There is also a need to raise awareness of the difference between risk management, insurance and safety management, especially in the mining and energy sectors.

This means that there is, therefore, a need to educate companies on the importance of enterprise risk management and encourage them to adopt enterprise risk management as a tool of value addition to the organisation. Buying insurance and sub-contracting are the main ways in which organisations transfer risks. There is a need for more research on how additional risk transfer markets can be created as the risk management profession matures in the region.

Smarntha Shonhiwa is a lecturer in the Department of Risk Management and Insurance, National University of Science and Technology, Bulawayo, Zimbabwe. David Chimsitu is a part-time Lecturer at National University of Science and Technology and member of the Institute and Faculty of Actuaries.

TOP RISK MANAGEMENT CHALLENGES IN ZIMBABWE

Changing perspectives

While the Black Lives Matter movement has pushed diversity onto the board agenda, most organisations will need to take proactive action if the enterprise is to benefit from a meaningful range of perspectives

BY IBI ESO

In the wake of George Floyd's killing in the US, many of the world's biggest brands have spoken out in support of black communities. The Black Lives Matter (BLM) movement has become part of everyday conversation but, while BLM is grabbing the news headlines, it is vital to recognise that diversity is also a much wider issue than skin colour or gender. It is also about having diversity of thought.

For most organisations, attaining this ideal will require nothing less than a deep-rooted overhaul of established, previously unquestioned practices. There are no quick fixes. The process must start at the top, from the board of directors down, as only they have the power to effect lasting cultural change.

Organisations wanting seriously to achieve diversity of thought cannot simply leave it to chance. They must make an active effort to bring people who look, behave and think differently to the boardroom table. Only by doing so can they avoid the dangers of groupthink – defined as "the practice of thinking or making decisions as a group, resulting typically in unchallenged, poor-quality decision-making".

> Those wanting seriously to achieve diversity of thought cannot simply leave it to chance

Groupthink

A commonly cited example of disastrous groupthink is Swissair, the airline that became so powerful and

> The wider the diversity of experiences, the wider the pool of knowledge that the team will bring to each decision, idea or project

financially stable that it earned the nickname "the Flying Bank". Over time, the board of directors came to believe themselves not only invulnerable to bad decisions but also morally superior to other companies. When the company restructured its board to achieve a more ideologically and strategically aligned group, it lost most of the board's industrial expertise, along with its alternative, opposing voices. The resulting groupthink eventually grounded a company that had been in business for 71 years and prompted its financial collapse in October 2001.

The spectacular rise and fall of blood-testing company Theranos, once valued at over $8 billion, is another cautionary tale on the dangers of groupthink. Its illustrious board featured former secretaries of state Henry Kissinger and George Shultz and retired general James Mattis. However, except for chief executive Elizabeth Holmes, the average age of the all-male board was 76 years. Critically, there was no diversity of expertise. Despite Theranos being a medical technology company, most of its directors were military officers, senators and former cabinet ministers – none of whom had any obvious medical or technology experience.

Better decisions

Board diversity matters but concentrating on only one form of diversity – gender, race and ethnicity or age – is not enough. Research by Stephanie Creary, assistant professor of management at the Wharton School, suggests that both social and professional diversity are crucial to increasing the diversity of perspectives represented on the board. This is easier to achieve when boards avoid filling open seats with people already in their personal and professional networks. A better approach is to periodically assess the skillset the board ideally needs, given its business and strategic direction, the skillset it already has and, in that way, identify the skills gap.

Encouraging diverse views to be heard improves decision-making and drives growth and innovation. The wider the diversity of experiences, the wider the pool of knowledge that the team will bring to each decision, idea or project, according to research by Antonia Hock, global head of The Ritz-Carlton Leadership Center. For example, alongside the traditional finance and operational viewpoints, this could involve appointing someone from human resources to the board to bring a different perspective or someone with the right skills but not from a traditional or commonly accepted background.

The board's culture is also a critical factor. It will come as no surprise that directors are more likely to share an opposing view when the board culture is open and collegiate, rather than hierarchical.

The value of the enhanced knowledge and experience of a diverse board was quantified by a further study by Cloverpop that found inclusive teams make better business decisions up to 87 per cent of the time. And that following a fully inclusive process means decisions are made twice as fast in half the number of meetings.

As for gender representation, decision-making improves as team diversity increases. Compared to individual decision-makers, all-male teams make better business decisions 58 per cent of the time, while gender-diverse teams do so 73 per cent of the time. Expanding on this, teams that also include a wide range of ages and different geographic locations make better business decisions 87 per cent of the time.

"This research highlights the potential value of team diversity as a practical tool for architecting decision-making processes," said Harvard Business School professor Francesca Gino. "That our decisions get side-tracked by biases is now well established. While it is hard to change how our brains are wired, it's possible to change the context of decisions by architecting the composition of decision-making teams for more diverse perspectives."

Mirroring communities

Why is it so important that an organisation's leadership reflects the communities it serves?

Firstly, it ensures services are shaped around its stakeholders. For instance, a charity that supports disadvantaged inner-city youth needs directors who mirror its clientele in terms of age, gender and background. A board consisting of comparatively wealthy, middle-class directors over retirement age, however well-meaning, simply cannot relate to the hidden challenges and obstacles their young stakeholders face daily.

However, it's vital not to make striving for diversity a tick-box exercise or resort to "tokenism" to achieve the required age, gender or ethnic balance. People should be recruited on the basis of the experience and knowledge they can add to board-level discussions.

STEPS TOWARDS DIVERSITY

Good practice includes:

- Striving to make your board composition representative of the demographic it serves
- Recognising that creating a diverse organisation starts with the recruitment process. Examine every step of the process to identify and remove potential barriers, for instance interview travel expenses
- Being conscious of the risk of stereotyping, whether by age, race, gender or family circumstances, and treating each candidate as an individual
- Implementing mandatory training to create awareness of equality and diversity issues among the workforce
- Considering conducting stakeholder analysis to increase the board's understanding of the organisation's stakeholders and strengthen the relationship
- Conducting regular analysis of changing patterns of behaviours and changes in the market
- Taking risk management seriously with a properly embedded risk management framework that helps to identify any risks and mitigations.

"A board consisting of comparatively wealthy, middle-class directors over retirement age, however well-meaning, simply cannot relate to the hidden challenges and obstacles their young stakeholders face daily

Unconscious bias

Secondly, diversity is needed to counter unconscious bias. This starts early – sometimes as early as primary school. To take just one small example of unwitting prejudice, most schools include hairstyle stipulations as part of their uniform policies. Many forbid students having haircuts shorter than a "number one", which is one-eighth of an inch. Yet this numbering system was developed with only Caucasians in mind and does not work for Afro-textured hair.

Then there is the difficulty many of us, including teachers, experience in pronouncing "foreign-sounding" names. We will often exaggerate mispronunciations in a misguided attempt to cover our embarrassment without realising this can be offensive to the individual concerned.

Organisations must be alert to such subtle examples of unconscious bias in our corporate culture. A Harvard Law School Forum on Corporate Governance by Adrianne Trainor and Byron Loflin explains this can range from blindness that causes boards to miss systemic issues to cultural norms, such as politeness, that discourage candour and constructive debate. Or "boards that prioritise particular skills, experience, knowledge and personal attributes when selecting new members, hoping to find 'a good fit'" – in other words, someone who looks, sounds and thinks like the board does.

Every organisation should review its policies with a questioning mindset to eliminate any inadvertent unconscious bias that could be prejudicial to any section of society.

Workplace diversity fosters mutual respect among employees. According to human resources expert Ruth Mayhew, when employees work in teams comprising co-workers with varied work styles, disabilities, or who represent different cultures or generations, a more tolerant work environment becomes the norm. The occasional disagreement aside, employees tend to recognise the strengths and talents that diversity brings to the workplace and they gain respect for their colleagues' performance.

In contrast, employees who don't see their identities reflected in the workplace feel a lower sense of belonging, which can lead to higher churn and lower productivity.

Bottom line

Building a diverse workforce isn't just the right thing to do. There is plenty of data to show that it increases the bottom line. Well before the watershed moment of George Floyd's death, a 2018 Edelman survey covering 35 countries showed that 64 per cent of consumers would buy from firms which they see as engaged in activism.

This is reinforced by a Boston Consulting Group study involving 1,700 companies in eight countries of varying sizes that demonstrated companies with more diverse management produce 19 per cent more revenue due to innovation. This finding is huge for tech companies, start-ups and, indeed, any business where innovation is the key to growth. It shows diversity is not merely a "nice to have" attribute that organisations should aspire to but an integral part of any successful revenue-generating business.

> **Employees tend to recognise the strengths and talents that diversity brings to the workplace and they gain respect for their colleagues' performance**

Risk management role

Risk management in its true sense will identify risks at the corporate governance level, for instance, a lack of succession planning or an unrepresentative board composition. It can ensure the organisation has a balanced board who can deliver the agreed strategy – and help directors avoid common pitfalls.

These include clumsy attempts to jump on the diversity bandwagon. Even the biggest companies can get it wrong. Pepsi, for example, was widely mocked for a notorious, tone-deaf advert featuring the celebrity Kendall Jenner, which appeared to trivialise BLM protests. Diversity is not about rushing to appease a certain group but opening up opportunities for all sections of society. But diversity will not happen by chance: it needs to be explicitly valued and proactively designed.

When businesses think narrowly about gender or racial diversity, this is limiting. As Lutfey Siddiqi, visiting professor-in-practice at LSE's Centre for International Studies, said, "This is not just the right thing to do. It is a stepping-stone to better governance."

Ibi Eso is a governance expert and managing director of Bridgehouse Company Secretaries, www.bhcsecretaries.co.uk. Eso is also IRM company secretary.

PITFALLS TO AVOID

- It is all too easy to subconsciously recruit candidates who match our own image. This will result in a uniformity of views – the very thing diverse organisations want to avoid. Aim to *remove subjectivity in recruitment or promotion decisions* to eliminate unconscious bias
- Avoid falling into the trap of words without action by *setting hiring targets and monitoring progress* towards them. Supplement this by asking grassroots staff and suppliers for their views in annual stakeholder surveys
- *Avoid groupthink*, starting from the top. A board that is not made up of suitably diverse people will end up with no challenges to decision-making or constructive discussions
- Don't view your organisation's strategy as being set in stone but *review and adapt it periodically* in the light of changes in the micro or macro landscape.

The future for energy

The pandemic has intensified pressures on the energy sector in its transition to a renewables future, according to a recent IRM report

The COVID-19 pandemic has hit the energy sector hard – at one stage sending oil prices spiralling into negative territory for the first time ever. But IRM's most recent report on the sector shows that the industry was already facing long-term challenges that have been exacerbated by the pandemic.

There are many threats to the sector made more complex and unpredictable by COVID-19. Energy consumption levels should plateau in 2030. Governments and consumers want renewables rather than fossil fuels. Geopolitical events continue to impact future commodity prices. Oversupply of oil is being made worse by shortages of storage facilities. Global supply chains are reshaping. And lockdowns are likely to make it difficult for businesses to meet the skills demands of the future while keeping the lights on today.

Prepared?

Given that many of these factors have been around for several years, some have asked why risk managers seemed unprepared for an event such as the pandemic. Up to 80 per cent of organisations surveyed by IRM said they did not have pandemic plans in place. The good news is that the unpredictable events and uncertainty related to the pandemic have highlighted the need for better crisis management planning in building strategic, operational and financial resilience across the business.

Improvements to energy industry organisations' future risk and resilience capabilities are under a renewed spotlight, borne out by the results of IRM's energy industry survey which show a significant move towards making improvements. Ninety per cent of respondents to the survey said they would actively seek to improve risk and resilience capabilities.

In fact, risk managers will play a greater role in bringing clarity to the evaluation and decisions on major new investments by providing input on financial, supply chain, digital, political and emerging risks, which could make or break the success of major investment programmes. Not only that, but risk management itself will need to evolve. That could include developing a new range of key risk indicators and better ways of monitoring risk factors in the external environment, which, as we have recently learned, can alter much more rapidly and dramatically than anticipated.

Plateau

Future energy use is expected to plateau by around 2030. This is expected to take place during a forecasted period of continuing economic growth while energy demand continues to increase but at a slower rate.

The most prominent anticipated change is the large-scale increase in electric vehicles, which is being driven by a combination of consumer behaviour, including increasing sensitivity to the environment, and governments pursuing agendas aimed at decarbonising their economies.

The current global situation during the COVID-19 pandemic has resulted in revised downward estimates of 5 per cent for electricity demand in 2020, the biggest drop since the 1930s (*IEA 2020, Global Energy Review 2020*). However, global electricity demand decreased by 2.5 per cent in the first quarter of 2020, even though lockdown measures were in place for less than a month in most countries. It will be some time before the total impact of COVID-19 can be fully assessed, especially since a milder European winter in 2020 needs to be accounted for.

Risk managers in the sector will have their work cut out over the coming years as energy companies adapt to the complex web of changes the world faces when it comes to keeping the lights on. With so many unpredictable factors at play, the risk department's focus on resilience is only likely to increase.

Read *Disruption, uncertainty and the role of risk management: IRM Energy and Renewables Special Interest Group Report*. https://bit.ly/3lloDWQ

Directory

Due diligence solutions

Enterprise risk management and risk analysis software

Governance, risk management, and compliance software

Integrated Risk Management

Riskonnect is the leading integrated risk management software solution provider. Our technology empowers organisations with the ability to anticipate, manage, and respond in real-time to strategic and operational risks across the extended enterprise. More than 900 customers across six continents use our unique risk-correlation technology to gain previously unattainable insights that deliver better business outcomes. Riskonnect has more than 500 risk management experts in the Americas, Europe, and Asia. To learn more, visit www.riskonnect.com

Mark Holt
+44 (0)7435 607 892
mark.holt@riskonnect.com
www.riskonnect.com
8 Lloyd's Avenue
London
EC3N 3EL

Reporting and compliance software solutions

Workiva Inc. (NYSE:WK), provider of the world's leading connected reporting and compliance platform, is used by thousands of enterprises across 180 countries, including 75 percent of Fortune 500® companies, and by government agencies. Our customers have linked over five billion data elements to trust their data, reduce risk and save time.

Tim Le Mare
+44 (0) 203 868 0550
info@workiva.com
www.workiva.com/uk
14 Gray's Inn Road
London
WC1X 8HN
United Kingdom

Risk management software

Since 2014, Origami Risk is the only company that has been consistently recognised for delivering client success, innovation, and stability, while 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, providing integrated solutions to the entire insurance value chain, serving Risk Managers, Brokers, TPAs and Carriers. 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) 16179 17740
nscotcher@origamirisk.com
www.origamirisk.com
30 Moorgate
London
EC2R 6PJ

Risk management software

In today's rapidly evolving world, business models and organisations are facing increased change and unprecedented levels of scrutiny. With change comes complexity, challenging risk managers to redefine the way they lead an organisation's approach to and implementation of risk management. Protecht helps organisations through deep understanding, monitoring and management of risk. We provide the complete risk solution—comprised of world-class enterprise risk management, compliance, training and advisory services—to government organisations, key regulators and businesses of all sizes across the world. With 20+ years at the forefront of risk and compliance solutions, millions of incidents managed across thousands of individual risks, and over 25 thousand people attending our training courses to date, we're one of the most respected and influential voices in risk.

Keith Davies
+44 (0) 7828 163 802
keith.davies@protechtgroup.com
www.protechtgroup.com
131 Finsbury Pavement
London
EC2A 1NT
United Kingdom

Risk management training

As the world's leading enterprise risk management institute, we know what great risk management looks like, and what risk management professionals need to know, do and deliver to succeed. What's more, we understand how training works and we are experts in designing and delivering courses that provide the tools and motivation to make change happen. Our short courses and tailored in-house learning and development solutions support hundreds of organisations every year, both in the UK and internationally. Some courses, like the Fundamentals of Risk Management, cover the broad range of ERM skills, whilst others take an in-depth look at specific topics, e.g. Risk Analysis, Risk Appetite and Tolerance, Managing Risk Culture, and Identifying Key Risk Indicators.

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

Why travel?

After months of being confined to home, our relationship to travel could be permanently different

Life has carried on the same for many key workers in the UK during the lockdown imposed during the height of the pandemic. But many more people have been stuck at home. Grocery deliveries, online shopping and other services that can arrive at the front door have soared. Road traffic volumes have plummeted – only recently edging back up to pre-pandemic levels.

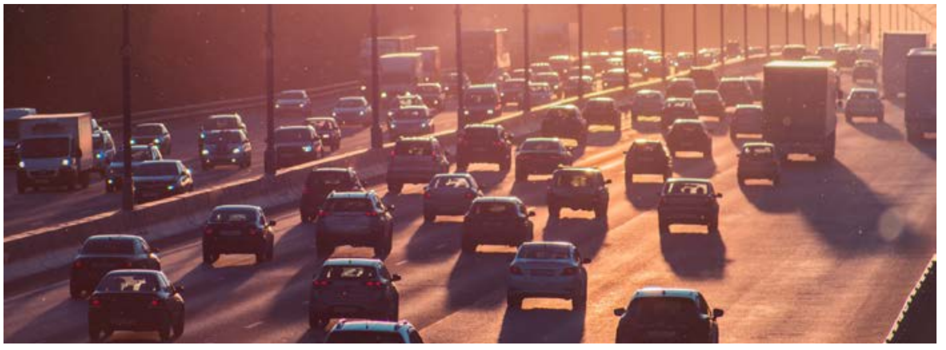
The travel industry is in chaos. Flight routes deemed safe by the government are being switched on and off faster than a broken traffic light. Travel for many people used to long daily commutes, regular international flights and foreign holidays has simply been cancelled.

Temporal landmarks

Defining essential travel during COVID-19 has thrown up the uncomfortable fact that so much of our to-ing and fro-ing is unnecessary. While online conference calls certainly have their downsides and awkward etiquette – how do you switch someone off politely? – they have the benefit of being efficient. Working from home is also hugely popular – almost 70 per cent of people said they would like to continue with it in a YouGov poll conducted earlier this year.

Permanent behavioural change often happens after a significant "temporal landmark", Katy Milkman, a behavioural scientist at the University of Pennsylvania's Wharton School, recently told *The Atlantic* magazine. "There's a mental time boundary –everyone's like, 'Whoa, in March of 2020, I opened a new chapter'– and we have this constraint [of social distancing] that forces us to explore new things. So, it's a double whammy." Several months is a long enough period for habits to change permanently, she said.

Image credit: Alexander Popov / Unsplash



> Milkman's research presents us with the uncomfortable suggestion that much travel is simply a bad habit

Bad habits

Milkman's research presents us with the uncomfortable suggestion that much travel is simply a bad habit: it is inefficient, unproductive, expensive and environmentally damaging. While there is no doubt some business travel is essential – checking out the culture in a failing plant overseas can reveal hidden and unexpected risks – technology can handle routine monitoring previously carried out by people. In the construction industry, for example, drones provide real-time data on aerial survey work, building safety and even help with construction work. The data from the drones' monitors can be fed back to anywhere in the world for analysis and decision making.

Was it even travel?

The rise of packaged holidays in the 1970s has been criticised for creating mass-produced experiences. There is nothing wrong with that – but does it really count as travelling in the more mind-expanding, romantic definition of the word?

In J-K Huysmans' turn-of-the-century novel *Against nature*, the protagonist Duc Jean Floressas des Esseintes decides to put himself in voluntary lockdown. He cuts himself off from the world in order to create the perfect, aesthetic living experience. Halfway through the project, he gets bored and decides to travel from Paris to England. On the way, he stops at a pub full of English people, orders English food and looks through the window at the rain-lashed streets. "When you come to think of it," he says, "I've seen and felt all I wanted to see and feel. I've been steeped in English life ever since I left home, and it would be madness to risk spoiling such unforgettable experiences by a clumsy change of locality." He returns home without ever setting foot in Britain. In other words, do you really need to travel to travel?

riskHive®

20 years of innovation delivered worldwide
enterprise risk management and analytics software

any risk any time anywhere

riskhive.com
ianbaker@riskhive.com
+44 1275 542839
+44 7818 898997